NATO OTAN

CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM



Terrorism in 2040

How to Counter Asymmetric Warfare in a Hyperconnected World



Edited by Christina Schori LIANG
Centre of Excellence Defence Against Terrorism
Ankara, Türkiye, 2026

E-ISBN: 978-975-409-814-3







TERRORISM IN 2040:
HOW TO COUNTER ASYMMETRIC WARFARE IN A HYPERCONNECTED WORLD

NATO COE-DAT
Research Project
Christina Schori LIANG
Editor

Centre of Excellence – Defence Against Terrorism
Ankara, Türkiye, 2026

Terrorism in 2040: How to Counter Asymmetric Warfare in a Hyperconnected World

LIANG, Christina Schori (ed.) 2026

İsmail Oğuz KARAMANLI, Project Coordinator, NATO COE-DAT

Authors: Richard Aldrich, John Arquilla, Vanda Felbab-Brown, Diana Paz Garcia, Justin Hastings, Lewis Herrington, Christina Schori Liang, Gergely Nemet, Giray Sadik, Erin Saltman.

First Edition, Ankara, September 2026

Published by

Centre of Excellence Defence Against Terrorism (COE-DAT)

Publisher Certificate Number: 47344

Address : Devlet Mahallesi İnönü Bulvarı Süleyman Emin Caddesi No:65 Çankaya 06582

Ankara – TÜRKİYE P.O. Box Address : P.K.-57 06582

Bakanlıklar-Ankara TÜRKİYE

PHONE : +90 312 425 82 15

FAX : +90 312 425 64 89

E-MAIL : info@coedat.nato.int

Printed by Öztepe Matbaacılık

Zübeyde Hanım Mahallesi Kazım Karabekir Caddesi No: 31/107 İskitler/ANKARA

Graphic Designed by Eray DEMİR and Ayberk AYHAN

© **All rights reserved by the Centre of Excellence Defence Against Terrorism**.

No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of COE-DAT.

Disclaimer

The information and views expressed in this book are solely those of the authors and do not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the authors are affiliated.

270 pages;
ISBN: 978-975-409-786-3

1. Asymmetric Warfare 2. Hyperconnected World 3. Counter Terrorism.

To cite this book: Christina Schori Liang (ed.) 2026, Terrorism in 2040: How to Counter Asymmetric Warfare in a Hyperconnected World – NATO COE-DAT Research Project - Ankara: Centre of Excellence Defence Against Terrorism

CONTENTS

Introduction
Dr. Christina Schori Liang,

Project Lead Researcher and Editor ……...1

Chapter 1: Key Global Trends Shaping NATO's Strategic Challenge to Counter Terrorism

Dr. Christina Schori Liang..... …….4

Chapter 2: What's Next for Terrorist Strategies?

Prof. John Arquilla 49

Chapter 3: Unconventional Terrorism: Future Trends in the Nuclear and Maritime Domains

Prof. Justin Hastings 66

Chapter 4: Transnational Terrorism in Africa: Mapping A New Role for NATO on the Continent

Dr. Christina Schori Liang..... 84

Chapter 5: Future of Terror-Crime Nexus

Dr. Vanda Felbab-Brown and Diana Paz Garcia 136

Chapter 6: Terrorists with Drones: Exploring the Effects of Lethal Autonomy on the Future of Counterterrorism

Prof. Dr. Giray Sadık 159

Chapter 7: Terrorist Recruitment and Online Social Engineering: Technology, Innovation and Future Global Trends

Prof. Richard J. Aldrich..... 171

Chapter 8: Future Terrorism, Extremism, and the Rise of Single-Issue Ideologies: Strategic Lessons from Ontological Security

Dr. Lewis Herrington..... 187

Chapter 9: Online Intervention Strategies for Preventing Youth Radicalization

Dr. Erin Saltman 224

Chapter 10: Strategic Foresight and Counter-Terrorism Futures: Aligning NATO Doctrine with Emerging Threats and Structural Drivers

Dr. Gergely Németh..... 245

Conclusions

The Next Battlespace: Multi-Domain Terrorism in a Hyperconnected World
Dr. Christina Schori Liang..... 272

Preface

The Centre of Excellence Defence Against Terrorism (COE-DAT) has been working for decades on projects that assist NATO strategic level decision makers by advice, doctrine, training and education addressing terrorism and counter-terrorism.

As a think tank for NATO the Centre made numerous efforts to forecast the future with workshops and researches that provided reports and research papers, books like “NATO and the Future of International Terrorism and Counterterrorism”, or “Future Trends in Insurgency and Countering Strategies” and “Emerging Threats in Terrorism”.

Understanding, that with every spin of the globe there are new challenges emerge like climate change, migration, technological development, etc. that bring conflicts, and affect the way and tools of the never-ending fight, our Centre tried again the impossible and looked deep in the “crystal ball”. With the help of great minds around the world year-long research, including workshops and lots of discussions, the team came to the conclusion manifested in this book with the aim and title of “Terrorism in 2040: How to Counter Asymmetric Warfare in a Hyperconnected World”.

The research demanded open mind and courage to look so far forward analyzing lessons and trends from the past, and establishing new perspectives and old-new trends and paint a picture of the possible future of fighting against terrorism.

The objective of this study that the findings will be not science-fiction read, but an outlook for strategists and planners of NATO and its partners that supports their long-term work building an Alliance equipped timely and well to counter the challenges.

I would also like to express my sincere appreciation to Gendarmerie Colonel Serkan KARAGÖZ, Colonel Tamas KENDER, Captain İsmail Oğuz KARAMANLI and all COE-DAT personnel for their dedicated efforts, professionalism, and valuable contributions throughout the preparation and completion of this project. Their commitment, coordination, and continued support played an important role in bringing this publication to fruition.

With the hope that our work has achieved the goal we envisioned I thank the team for their incredible work and wish you Dear Readers that you find this book a useful read.

Halil Sıddık AYHAN
Colonel (TUR A)
Director, COE-DAT

Acknowledgments

The Centre of Excellence Defence Against Terrorism (COE-DAT) is proud to complete this book to address Terrorism in 2040: How to Counter Asymmetric Warfare in a Hyperconnected World. The topics captured in this project represent a deep dive in the understanding of the future and its challenges and more importantly, it offers NATO Allies and partner valuable recommendations to address the possible emerging threats and enhance the effectiveness of counter-terrorism efforts.

I would like to express our gratitude to the researchers including Richard Aldrich, John Arquilla, Vanda Felbab-Brown, Diana Paz Garcia, Justin Hastings, Lewis Herrington, Gergely Német, Giray Sadık and Erin Saltman for their invaluable support and our special thanks to Christina Schori Liang for leading of this project that made this book a reality.

Last but not least, my gratitude goes to the COE-DAT staff for their dedication and professionalism that ensured the success of this project.

Tamas KENDER
Colonel (HUN A)
Knowledge Department Chief
COE-DAT

DISCLAIMER

The edited book is a product of the Centre of Excellence-Defence Against Terrorism (COE-DAT). It is produced for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. It does NOT represent the opinions or policies of NATO, COE-DAT or the framework and sponsoring nations of COE-DAT. The views and terminology presented in the book are those of the authors.

BIOGRAPHIES OF THE EDITOR AND AUTHORS

Project Manager & Editor

Dr. Christina Schori Liang is Head of Counterterrorism and Preventing Violent Extremism at the Geneva Centre for Security Policy (GCSP) in Geneva, Switzerland. At GCSP, she delivers courses on Preventing Violent Extremism and Transnational Organized Crime. Dr. Liang leads GCSP's monthly *Geneva Security Debates* which feature the world's leading thinkers on important security challenges. Dr Liang is a prolific writer and has given over a hundred academic and policy-related presentations in 40 countries. Dr. Liang is the editor of *Europe for the Europeans: The Foreign and Security Policy of the Populist Radical Right* and a long-standing contributor to the *Global Terrorism Index* published by the Institute for Economics and Peace, with contributions spanning from 2015-2025.

Dr. Liang serves on the Scientific Board of the NATO Defense College Foundation and is a member of the Partnership for Peace Consortium's Irregular Warfare and Hybrid Threats Working Group. She has taught university courses for more than 25 years, including at Boston University, and currently teaches at the Paris School of International Affairs (PSIA) at Sciences Po, where she serves as an Adjunct Professor in the Global Risks and Intelligence Studies departments. Dr. Liang holds a doctorate in International Relations from the Graduate Institute of International and Development Studies in Geneva, Switzerland.

Author Biographies[1]

Prof. Richard J. Aldrich is a Professor of International Security at the University of Warwick and a Fellow of the Royal Historical Society. He has served as co-lead for the Warwick Cybersecurity Global Research Priority and in 2018 received the ISA Distinguished Scholar Award from the Intelligence Studies Section. His publications include *The Black Door: Spies, Secret Intelligence and British Prime Ministers* (2016) and *GCHQ* (2019). He is currently completing a book on *AI, Cybersecurity and Digital Politics* for Oxford University Press. His articles have appeared in *International Affairs*, *Foreign Affairs*, *Foreign Policy* and *West European Politics*. He has recently been involved with the H2020 DigiGen project on digital youth in Europe, together with the Jean Monnet Erasmus 'Cydiplomacy' scheme.

Prof. John Arquilla is Distinguished Professor Emeritus at the United States Naval Postgraduate School, where he taught courses in irregular warfare and the impact of technology on military affairs from 1993 -2021. He is best known for having

[1] The authors are listed in alphabetical order by their last names.

co-developed the concepts of cyberwar, netwar, and swarm tactics with his RAND colleague David Ronfeldt. His books include: *Networks and Netwars: The Future of Terror, Crime, and Militancy* (2001); *Insurgents, Raiders, and Bandits* (2011); and *Bitskrieg: The New Challenge of Cyberwarfare* (2021). Dr. Arquilla's policy experience has extended to consulting senior leaders across a range of events, from Desert Storm to the Kosovo War, and in various post-9/11 matters.

Dr. Vanda Felbab-Brown is a senior fellow in Foreign Policy at the Brookings Institution. She is also the director of Brookings' Initiative on Nonstate Armed Actors and of the Brookings series the Fentanyl Epidemic in North America and the Global Reach of Synthetic Drugs and co-director of the Africa Security Initiative at Brookings. Dr. Felbab-Brown is an expert on international and internal conflicts, insurgency, terrorism, urban violence, organized crime, and illicit economies. Her fieldwork has covered Afghanistan, South Asia, Myanmar, Indonesia, the Andean region, Mexico, Iraq, Somalia and the Horn of Africa, Nigeria and West Africa, and other African regions.

She is the author of five books - *Narco Noir: Mexico's Cartels, Cops, and Corruption* (forthcoming); *The Extinction Market: Wildlife Trafficking and How to Counter It* (2017);

Militants, Criminals, and Warlords: The Challenge of Local Governance in an Age of Disorder (2017; co-authored); *Aspiration and Ambivalence: Strategies and Realities of Counterinsurgency and State-Building in Afghanistan* (2013); and *Shooting Up: Counterinsurgency and the War on Drugs* (2010) as well as many policy reports, articles, and opeds.

Dr. Felbab-Brown has been a consultant for various U.S. government agencies and has served on several U.S. high-level government advisory boards on matters of national security and U.S. foreign policy. She frequently testifies in the U.S. Congress. She also regularly serves as an expert witness in U.S. criminal and civil cases involving matters of organized crime and illicit economies. In 2020 and 2021, Dr. Felbab-Brown also served as a senior advisor to the congressionally-mandated USIP Afghanistan Study Group. Dr. Felbab-Brown has also worked as a consultant for NATO, the World Bank, the United Nations, and the governments of Canada and the United Kingdom. A recipient of numerous awards, Dr. Felbab-Brown received her Ph.D. in political science from MIT and her B.A. in government from Harvard University.

Diana Paz García is an international conflict analyst specializing in nonstate armed actors and gender-based violence. She is a Senior Research Assistant at the Brookings Institution, where she coordinates *The Fentanyl Epidemic in North America and the Global Reach of Synthetic Opioids* project and conducts research on organized crime, terrorism, and illicit economies worldwide. Diana has served as an

advisor and consultant for the Mexican Dirty War Commission, Nadia's Initiative, Oxfam America, and Winrock International, focusing on international security, transitional justice, and conflict-related sexual violence. She holds an M.A. in Conflict Resolution from Georgetown University and a B.A. in Political Science and International Studies from Macalester College.

Prof. Justin V. Hastings is Professor of International Relations and Comparative Politics at the University of Sydney in Australia. He is the author of three books -- *No Man's Land: Globalization, Territory, and Clandestine Groups in Southeast Asia* (Cornell University Press, 2010), *A Most Enterprising Country: North Korea in the Global Economy* (Cornell University Press, 2016), and *On the Seas of the Indo-Pacific: Rogue Strategies and Maritime Security Threats* (Edinburgh University Press, forthcoming 2027) – as well as over 150 other research publications, including in journals such as *International Studies Quarterly*, *Security Studies, Journal of Peace Research, American Journal of Agricultural Economics, Terrorism and Political Violence, Small Wars and Insurgencies, Political Geography,* and the *Review of International Political Economy*. Hastings' research has been funded by the Australian Research Council, the MacArthur Foundation, the National Bureau of Asian Research, the US-Indonesia Society, the US Department of Defense, the Australian Defence Department, and the Korea Foundation, among others. His research on terrorism has covered maritime terrorism, CBRN terrorism, the political economy of terrorism, the nexus between terrorism and organised crime, the impact of geography and technology on the structure and behaviour of terrorist organisations, and the connection between food production, climate, and armed conflict, primarily but not exclusively in the Indo-Pacific. He holds an AB in public and international affairs from Princeton University, and an MA and PhD in political science from the University of California, Berkeley.

Dr. Lewis Herrington is an interdisciplinary scholar whose work examines terrorism, radicalisation, political violence, cognitive warfare and the psychological foundations of extremist behaviour. He holds a PhD in terrorism studies from the University of Warwick, where his ESRC-funded research drew on court records, ethnographic evidence and interviews with former Cabinet ministers, intelligence professionals and serving counter-terrorism officers. He also holds postgraduate qualifications spanning computer science, politics and psychology, enabling him to connect technological, political and behavioural approaches to contemporary security.

He is the author of a monograph on understanding terrorism in Europe published by Routledge, 2022, which develops new explanations of radicalisation and suicide terrorism through detailed analysis of European attackers. His research has appeared in leading journals, including *International Affairs*, *Intelligence and National Security*, *Review of International Studies* and *Politics*, and has addressed subjects ranging from British extremism and counter-radicalisation to hostage policy, cyber-

resilience and the changing terrorism landscape. His work combines archival sources, elite interviews and psychologically informed case analysis to explain transitions from extremism to violence.

Dr Herrington formerly served as Lecturer in International Relations at Coventry University, following teaching appointments at Warwick, Loughborough, Regent's and Buckingham universities. His research has informed engagement with government and counter-terrorism practitioners, including the UK Office for Security and Counter Terrorism and the Foreign and Commonwealth Office, and he has advised organisations supporting individuals vulnerable to radicalisation. He has also provided expert analysis for major international media outlets, including the BBC, CNN and Sky News.

His current research brings together political psychology, neuroscience, artificial intelligence and security studies to investigate ontological insecurity, single-issue extremism and the emerging use of personalised digital influence in cognitive warfare. A central concern of his work is translating interdisciplinary theory into practical strategies for prevention, democratic resilience and counterterrorism.

Dr. Gergely Németh since September 2024, he serves as the Chief Executive Officer of the Defence Innovation and Research Institute, where he drives innovation in defense technologies and oversees strategic research initiatives aimed at enhancing Hungary's defense capabilities. Prior to his current role, Németh was the Head of Strategic Foresight at NATO Supreme Allied Command Transformation in Norfolk, Virginia. In this position, he led the development of the Strategic Foresight Analysis, where he and his team of experts assessed the implications of future technology landscapes, threats, and challenges.

Before joining NATO's Strategic Foresight team, Németh served as the Director for Defense Policy at the Hungarian Ministry of Defense (MoD). In this capacity, he directed international relations, policy, and planning for the Ministry, including the formulation of the Hungarian National Military Strategy (2021) and the Hungarian National Security Strategy (2020). Additionally, as Deputy to the National Armament Director, Németh managed international affairs, including government-to-government (G2G) and government-to-business (G2B) relations, with a focus on technology and defense procurement.

Dr. Németh has also served as Deputy Defence Counsellor at NATO Headquarters in Brussels, where he contributed to the development of critical NATO initiatives such as the Defence Investment Pledge, Readiness Action Plan, and Graduated Response Plans. Earlier in his career, he served as a senior defense planning expert at the Hungarian MoD and spent four years as an analyst at J5

Hungarian General Staff. Dr. Németh holds a PhD in War Studies. He is married and the father of three.

Prof. Dr. Giray Sadık is a Full-Professor and Chair in the Department of International Relations, Faculty of Political Science (SBF), and Director of European Studies Research Center (AVAR), both of them at Ankara Yıldırım Beyazıt University, Türkiye. Previously, he was *Eisenhower Fellow* at NATO Defense College, Rome, Italy, and Swedish Institute Postdoctoral Fellow in the Department of Global Political Studies at Malmö University, Sweden. Prof. SADIK received his PhD in Political Science from the University of Georgia, USA, specializing in International Relations and Comparative Politics. His current research focuses on international security, hybrid threats, Transatlantic relations, counter-terrorism, European security and foreign policy, the use of technology for border and maritime security including Emerging Disruptive Technologies such as AI and UMS. Prof. SADIK is a member of the *Expert Pool of the European Center of Excellence for Countering Hybrid Threats*, Helsinki, Finland. Prof. SADIK was a guest lecturer and invited speaker on international security issues at various international forums including Carleton University (Canada), Baltic Defense College (Estonia), NATO School Oberammergau (Germany), NATO Maritime Security Centre of Excellence (MARSEC, Türkiye), London School of Economics and

Political Science (UK), European Policy Center (Belgium), Rondeli Security Conference (Georgia), Zagreb Security Forum (Croatia), and *Ludovika Fellow* at National University of Public Service (Hungary).

Dr. Erin Saltman is the President and CEO of the Tech Coalition, uniting the global tech industry to protect children online. Throughout her career she has collaborated with global multistakeholder partnerships, building out online policies and intervention programs in partnership with the tech industry, government, and civil society. Dr. Saltman was previously the Senior Director of Membership & Programs at the Global Internet Forum to Counter Terrorism (GIFCT) and was Meta's former Head of Dangerous Organizations Policy for Europe, the Middle East and Africa.

Dr Saltman holds a PhD from University College London (UCL) in political science. She holds a dual MA from UCL and Corvinus University as an Erasmus Mundus Scholar. She completed her BA in International Relations from Columbia University. technology, NGO, and academic sectors, building out international counterterrorism strategies and programs. Dr. Saltman’s background and expertise includes analyzing processes of radicalization within a range of regional and socio-political contexts. Her research and publications have focused on the evolving nature of violent extremism online, youth radicalization, and the evaluation of positive intervention tactics. At GIFCT, Dr. Saltman leads membership work with global technology companies and multistakeholder knowledge-exchange programs. She was

formerly Meta’s Head of Counterterrorism and Dangerous Organizations Policy across Europe, the Middle East, and Africa. Dr. Saltman is a graduate of Columbia University (BA), Corvinus University (MA) and University College London (MA and PhD).

TERRORISM IN 2040: HOW TO COUNTER ASYMMETRIC WARFARE IN A HYPERCONNECTED WORLD

INTRODUCTION

Dr. Christina Schori Liang

Project Lead Researcher and Editor

COE-DAT Project on *Terrorism in 2040: How to Counter Asymmetric Warfare in a Hyperconnected World*

The question of what terrorism will look like in 2040 looms large not only in the minds of intelligence professionals, military planners, policymakers, and scholars, but also among those charged with safeguarding the resilience of democratic societies in an era of profound geopolitical, technological, and societal transformation. Terrorism has never been a static phenomenon, throughout modern history, it has continuously adapted to political change, exploited technological innovation, and evolving alongside shifting patterns of conflict and war. As NATO prepares for an increasingly complex strategic environment, understanding the potential futures of terrorism is not simply an academic exercise; it is a strategic necessity.

Forecasting terrorism is inherently fraught with uncertainty. Few security actors have demonstrated such remarkable agility and adaptability. Terrorist organizations have repeatedly defied predictions of their decline, reinventing themselves in response to military pressure, political opportunity, ideological competition, and technological disruption. The global resurgence of religiously motivated extremist movements following the Cold War, the proliferation of decentralized extremist movements through social media, the rise of self-radicalized actors, and the convergence of criminal and terrorist networks all illustrate that terrorism evolves not according to linear trajectories but through complex interactions between social, political, economic, and technological forces.

The year 2040 lies at the intersection of several transformative trends that will reshape both the opportunities available to terrorist actors and the vulnerabilities of the societies they seek to influence. Advances in artificial intelligence, autonomous systems, biotechnology, quantum technologies, cyber capabilities, synthetic media, and ubiquitous connectivity are likely to alter the operational environment fundamentally. At the same time, climate change, demographic shifts, rapid

urbanization, migration, resource competition, strategic rivalry among major powers, and changing patterns of governance will create new contexts within which terrorism may emerge, adapt, and flourish.

These developments suggest that the future threat landscape cannot be understood solely by extrapolating from today's terrorist organizations. The most dangerous threats of 2040 may not resemble the hierarchical groups that dominated the early twenty-first century. Instead, future terrorism may be characterized by fluid networks, hybrid actors operating across physical and virtual domains, highly personalized radicalization pathways, and increasingly sophisticated exploitation of emerging technologies. Some actors may seek mass casualties through novel means, while others may prioritize disruption, psychological coercion, economic paralysis, or attacks against the digital infrastructure upon which modern societies increasingly depend.

Equally important is the recognition that terrorism does not exist in isolation from broader strategic competition. The boundaries separating terrorism, insurgency, organized crime, cyber operations, information warfare, and state-sponsored coercion are becoming progressively less distinct. Non-state actors may increasingly benefit from technologies once available only to states, while state actors may find value in exploiting terrorist proxies or extremist ecosystems as instruments of strategic competition. Such convergence complicates traditional legal frameworks, intelligence collection, attribution, deterrence, and collective defense.

For NATO, these evolving dynamics raise fundamental questions. How should the Alliance prepare for terrorist threats that exploit emerging technologies? How can collective resilience be strengthened against attacks targeting critical infrastructure, supply chains, information environments, and democratic institutions? What capabilities, partnerships, intelligence structures, and operational concepts will be required to anticipate threats that may emerge simultaneously across cyber, physical, cognitive, and space domains? Perhaps most importantly, how can NATO cultivate strategic agility in a future where surprise itself has become a defining feature of security?

This volume approaches these questions through the lens of strategic foresight rather than prediction. It does not seek to identify a single, definitive future for terrorism. Instead, it explores multiple plausible futures, recognizing that uncertainty is itself a defining characteristic of the strategic environment. Strategic foresight enables decision-makers to identify emerging trends, challenge assumptions, examine weak signals, and test policies against a range of possible futures before they materialize. In doing so, it strengthens preparedness without claiming certainty.

The chapters that follow examine the drivers likely to shape terrorism through 2040, including technological innovation, geopolitical instability, ideological evolution, societal polarization, environmental pressures, and changing patterns of conflict. They assess how these drivers may interact to produce new terrorist capabilities, organizational models, operational methods, and strategic objectives. Equally, they will consider what implications this will have for NATO's deterrence posture, force development, intelligence cooperation, partnerships, counterterrorism strategy and resilience.

The central argument of this book is straightforward but consequential: terrorism in 2040 will almost certainly look very different from the threats we face today—just as today's threats differ significantly from those of twenty years ago. Preparing for that future demands more than improved intelligence or enhanced operational capabilities. It requires imagination disciplined by rigorous analysis, an appreciation of complexity, and a willingness to challenge established assumptions before events compel change. In an age defined by accelerating technological innovation and strategic uncertainty, the greatest risk may not be failing to predict the future precisely but failing to prepare for futures that are both plausible and profoundly consequential.

This book is intended to contribute to that effort. By examining how terrorism might evolve through 2040, it seeks to inform strategic dialogue across the Alliance and among its partners. Its aim is to foster a shared understanding of the challenges ahead and, more importantly, of the choices that must be made today to strengthen security in an increasingly uncertain future.

CHAPTER 1

Key Global Trends Shaping NATO's Strategic Challenge to Counter Terrorism

Dr. Christina Schori Liang

Abstract

Technology will shape our future in more ways than we can imagine—not only transforming the world around us but also redefining who we are and what we are capable of becoming in the coming decades. The NATO alliance will face significant challenges stemming from five major global trends: rising national populism; profound transformations in the technological landscape; innovations in next-generation warfare; the resurgence of great-power competition; and the increasing fragmentation of the rules-based international order. The rapid democratization of advanced technologies is revising the terrorist threat by empowering non-state actors with capabilities once reserved for states. Increasingly AI-enabled technologies that are accessible and affordable have improved terrorists' ability to communicate, recruit, finance, and disseminate propaganda and their ability to conduct cyber-enabled and physical attacks. The convergence of artificial intelligence, encrypted communications, cryptocurrencies, and commercial drones is reinforcing the asymmetric nature of terrorism. Technological power is increasingly distributed across a new security axis comprising of states, private industry, and influential technology leaders, fundamentally reshaping NATO's strategic environment. A growing reliance on private digital infrastructure creates new vulnerabilities that will require technological leadership to preserve NATO's strategic advantage in countering future terrorist threats. Collectively, these dynamics will reshape the strategic environment in which NATO operates and place growing strain on its existing doctrines and institutional capacities.

Introduction

Over the coming twenty years, the NATO alliance will face significant challenges stemming from five major global trends: rising national populism; profound transformations in the global technological landscape; innovations in next-generation warfare; the resurgence of great-power competition; and the increasing fragmentation of the rules-based international order. These developments will significantly affect NATO's ability to counter terrorism threats. Moreover, NATO—along with the broader Westphalian system of global governance—is ill-equipped to manage these emerging

trends in isolation and will therefore need to cultivate new partnerships and develop new institutional frameworks to adapt to this evolving reality.

The first trend is the ascent of national populism**.** In the current geopolitical landscape an increasing number of governments are adopting inward-looking approaches, emphasizing domestic resilience and sovereignty over sustained global engagement. This trend marks an increasingly widening globalist/nationalist divide that is intensifying in severity within multiple nation states. The rise of national populism is closely linked to deeper structural drivers – declining trust in public health, international institutions as well as cultural anxiety linked to globalization, immigration and economic security. This inward shift has fragmented the global order, weakening collective international governance, the NATO alliance and the former cooperative frameworks that once helped manage transnational threats including the meteoric rise of global terrorism in 2001.

This nationalist/globalist divide is separating states into two groups: those that want national interests to prevail and those that seek global, international solutions to problems. This growing internal political churn within states makes them more politically polarized and creates conditions conducive to extremist ideologies that help feed extremist and terrorist groups.

In the NATO context, national populism frequently manifests as skepticism toward international institutions, resistance to burden-sharing obligations, and criticism of what are portrayed as distant or unaccountable transnational elites. Populist leaders may exploit this narrative to question alliance commitments and limit military engagement abroad. For NATO, this framing can erode public support for collective defense by portraying the Alliance as an external constraint on national autonomy rather than a guarantor of democratic resilience and security.

Moreover, adversarial actors can exploit populist narratives through disinformation and hybrid tactics, amplifying societal polarization and weakening alliance cohesion from within. These dynamics directly impact societal resilience, democratic legitimacy, and the willingness of member states to sustain long-term security investments. As a result, NATO's long-term effectiveness will hinge on its ability to use strategic communication to strengthen the Alliance's democratic foundations, clearly convey its concrete security benefits, and sustain unity, credibility, and collective resolve among its members.

The second trend relates to the global technological landscape which is undergoing significant shifts, propelled by fast-moving innovations in technology. This trend must be situated within a global technological landscape undergoing profound transformation, driven by rapid advances in cyberspace, artificial intelligence (AI), drones, space systems, the Internet of Things (IoT), 5G communications, and subsea

data cables. These domains are of particular importance to nation states and violent non-state actors.

Together, these technologies constitute the backbone of the digital infrastructure that will underpin economic growth, governance, and security in the twenty-first century. This digital architecture consists of overlapping platforms and infrastructures controlled by a wide range of public and private actors, creating an interconnected ecosystem that transcends national borders. Digital assets are not governed by territoriality; even when equipment is physically located within a state, it flows through transnational, non-physical networks that defy physical reach. As a result, cyberspace inherently obscures the origin and attribution of hostile acts, introducing ambiguity that weakens accountability and a state's regulatory authority. States face the challenging task of responding to malware authored in one location, deployed globally via automated systems, routed through anonymizing networks, or via botnet devices scattered across numerous jurisdictions (Kello, 2017).

Terrorist organizations have increasingly exploited this environment to enhance their reach and resilience. Groups such as DAESH and Al-Qaeda have used encrypted messaging platforms like Telegram and online forums to disseminate propaganda, coordinate supporters, and inspire attacks across continents with minimal risk of interception.

DAESH has also demonstrated how digital platforms can enable decentralized operations, allowing sympathizers to act independently while remaining ideologically connected to the organization (Conway, 2017). In the cyber domain, terrorist-linked actors have conducted website defacements and disruptive cyberattacks, such as the 2015 attack on the French TV network TV5Monde, which was attributed to individuals linked to DAESH (Europol, 2016). In 2025, a new Al-Qaeda-affiliated hacker group known as the *Cyber Jihad Movement* emerged and began launching coordinated cyberattacks against Israeli and U.S. digital infrastructure as part of its broader ideological campaign, demonstrating how extremist organizations are now creating dedicated cyber units to target perceived enemies online (UNODC, 2024, CSIS 2025). These examples illustrate how terrorists benefit from the borderless, opaque nature of cyberspace, leveraging anonymity, global connectivity, and weak governance to project influence and conduct operations far beyond their physical presence (Nye, 2011).

The third trend has been the wide-ranging innovations in new generation warfare. The transformation of modern warfare is no longer simply tactical but structural, demanding a reassessment of military doctrine, international legal frameworks, and the nature of state authority in the 21st century(Krepinevich, 1994). As precision technologies become increasingly accessible and autonomous systems

grow more advanced, a central challenge will be ensuring meaningful human control over the use of force while upholding the humanitarian norms and principles that have underpinned international relations for more than a century (Schmitt, 2019).

The Russia–Ukraine war, which began in February 2022, simultaneously reflects the strategic heritage of past global conflicts while integrating the technological breakthroughs of new generation warfare (Freedman, 2022). In the early stages of the invasion, Russian forces employed armored columns classic military tactics of the first World Wars, followed by advancing infantry formations (Galeotti, 2022). However, the character of the conflict shifted dramatically with the introduction of unmanned aerial systems—both reconnaissance and combat drones—which altered surveillance, targeting, and strike dynamics across the battlespace (Bronk, Reynolds, & Watling, 2023). Ukraine's Operation Spider's Web stands out as a highly effective covert operation with implications that extend well beyond the Russia-Ukraine war. Using 117 low-cost drones covertly transported deep into Russian terrain it remotely operated the attack on several Russian airbases. Ukraine reportedly damaged or destroyed 41 aircraft, including bombers that carry strategic missiles, inflicting up to 7 billion dollars in losses a fraction of the cost of the operation (RUSI, 2024, Bego, 2025).

Modern conflicts demonstrate how technological advances are not only changing battlefield tactics but are also increasing the asymmetric nature of warfare and hybrid warfare (Hoffman, 2007). What once constituted the playbook of the weak mostly used by violent non-state actors ranging from rebel groups to terrorists has increasingly been adopted —and refined—by major powers, marking a profound shift in the character of contemporary conflict (Kaldor, 2012). Ukraine's Operation Spider's Web will undoubtedly enter the history books as one of the most remarkable and best-executed covert operations of the war, with potential consequences for warfare far beyond the current conflict(RUSI, 2023).

The war in Ukraine is showcasing innovative tactics, technological advancements, and asymmetric strategies. As with previous conflicts, terrorist groups worldwide are closely observing these developments, drawing valuable lessons to enhance their own capabilities. From drone warfare to cyber-attacks, the Russia-Ukraine war is reshaping the landscape of modern terrorism, equipping non-state actors with new tools and techniques to challenge conventional security measures (Liang, 2025).

Terrorist groups are increasingly absorbing lessons in asymmetric warfare from the strategies employed by major powers such as Russia, China, and the United States (Hoffmann, 2007). By observing how these states use hybrid tactics, cyber operations, information warfare, and low-cost technologies to their advantage terrorist organizations are refining their operational playbooks (Kaldor, 2012). Russia has

operationalized asymmetry through the weaponization of social media to shape information environments and, according to multiple Western assessments, influence foreign electoral processes, while simultaneously deploying so-called “little green men” during the annexation of Crimea from Ukraine in 2014 (Galeotti, 2016). These deniable, unmarked forces were deliberately designed to obscure attribution and blur the boundary between war and peace (Freedman, 2018). The subsequent use of mercenary formations such as the Wagner Group (renamed Africa Corps) extended this logic beyond Europe, enabling Moscow to project power in Africa and the Middle East while maintaining plausible deniability and avoiding the political costs of overt military intervention (Hoffmann, 2021). These methods reflect a futuristic, hit-and-run style of warfare in which influence operations, proxy forces, and ambiguity achieve strategic effects without the formal declaration of war or the large-scale deployment of conventional forces (Rid, 2016).

China has pursued a parallel but distinct asymmetric approach by fusing state authority with private industry through its doctrine of civil–military fusion**,** particularly in cyberspace and the information domain (Cheung, 2017). Rather than relying on kinetic force, Beijing has leveraged intellectual property acquisition, cyber espionage, and digital influence campaigns to shape international narratives and accelerate technological development to advance its long-term strategic objectives (Lewis, 2018). These methods allow China to contest power incrementally, operating below the threshold of armed conflict while reshaping the strategic environment in its favor (Polyakova, Meserole, 2019).

The United States—traditionally positioned as a target of asymmetric tactics—has employed comparable instruments, using cyber operations such as the Stuxnet operation as a coercive tool capable of imposing strategic costs without direct military confrontation (Zetter, 2014). In this new contemporary geopolitical competition, the United States has increasingly relied on asymmetric instruments of statecraft to shape the strategic behavior of rivals such as Russia and China (Nye, 2012). Rather than engaging in direct military confrontation, Washington has leveraged economic statecraft—notably sanctions, export controls, and financial restrictions—to impose systemic costs on adversaries while avoiding conventional warfare (Baldwin, 2016). Sanctions regimes targeting Russia’s financial sectors, energy exports, and key industrial capacities after Moscow’s incursions into Ukraine exemplify how economic leverage functions as an asymmetric tool of coercion, compelling adversaries to bear sustained economic pain without escalating to open conflict (O’Boyle, C. & Lanoszka, 2022).

The United States has similarly employed targeted export controls on advanced semiconductors and related technologies to constrain China’s access to critical components necessary for artificial intelligence and high-end computing, reflecting a

strategy designed to shape the technological terrain of competition rather than achieve battlefield dominance (US Dept. Commerce, 2023). Along with these economic measures, the U.S. has integrated cyber-enabled and informational asymmetric practices as exemplified by the United States' preemptive disclosure of Russian military intentions prior to the 2022 invasion of Ukraine, which sought to counter Moscow's misinformation campaigns and shape international perceptions (Polyakova & Meserole, 2022). Together, these cases illustrate how asymmetric methods now enable states to achieve geopolitical objectives without firing a single shot**,** relying instead on deniability, disruption, and political and economic influence (Rid & Buchanan, 2022).

This is happening against a backdrop of a fourth trend intensifying geopolitical competition, as states and corporations vie for primacy in the development and deployment of the most strategically significant technologies. China and the United States are locked in an intensifying geopolitical struggle for technological dominance, with digital infrastructure emerging as a central arena of strategic competition. As states race to harness accelerating digitalization, demand for affordable digital infrastructure and services has surged—particularly in emerging markets where connectivity, cloud services, and smart systems promise significant developmental gains.

Within this context, Washington and Beijing are competing to shape the digital futures of strategically important "swing" states. The stakes extend far beyond market share: entire regions risk becoming embedded within China-centric digital ecosystems, reinforcing Beijing's leadership in critical technologies while enabling the global diffusion of techno-authoritarian governance models characterized by pervasive surveillance, centralized data control, and limited transparency or accountability (Minvielle, Rousie and Thomas, 2025).

Crucially, this competition also carries implications beyond state-to-state rivalry, particularly with regard to violent non-state and terrorist actors (Nye, 2011). Where the United States and its allies tend to emphasize regulatory controls, export restrictions, and counterterrorism safeguards around advanced technologies, China's governance and export approaches toward emerging technologies differ significantly from those of Western regulatory frameworks, particularly regarding oversight of how such technologies may be repurposed by terrorists, extremists, or criminal networks (Cheung, 2022). These differences should primarily be understood within the broader context of competing governance models and varying approaches to digital sovereignty, regulation, and technological development. As a result, when advanced digital infrastructure—such as low-cost 5G networks, AI-enabled surveillance tools, satellite services, or IoT platforms—is exported without robust governance

frameworks, it may become accessible not only to partner governments but also to non-state actors operating within those ecosystems (Segal, 2018).

Weak oversight, authoritarian tolerance of coercive digital practices, and blurred boundaries between state and private industry can create permissive environments in which extremist groups exploit advanced technologies for propaganda, surveillance evasion, fundraising, or disruption (Weimann, 2015). In this sense, technological diffusion that bypasses U.S.-led norms does not merely shift geopolitical influence; it potentially lowers the barriers for extremist misuse of cutting-edge tools (Polyakova, & Meserole, 2019).

Great-power disorder helps terrorists because great power rivalries have become a great distraction for many countries. (Hoffmann, 2007) Nations such as China, Russia and the USA are investing and diverting their resources and attention to great-power politics. (Allison, 2017) Allocating their military, intelligence, and diplomatic capacity toward great-power competition (deterring China, responding to Russia, blocking the USA). Given this new agenda fewer resources remain to oversee counter-terrorism cooperation, capacity-building, and intelligence sharing — creating wide gaps terrorists can exploit (O'Boyle, C. & Lanoszka, 2022). Security actors from both the intelligence and defense community have repeatedly warned that competing priorities reduce counter-terrorism bandwidth (Clarke & Knake, 2019).

This intensifying geopolitical rivalry is giving rise to a fifth global trend: the erosion of multilateralism, resulting in the fragmentation of international norms and a decline in global cooperation. This geopolitical rivalry places significant strain on alliances and international institutions, complicating the establishment of new norms, soft law, coordinated sanctions, legal designations, and collaborative law enforcement. As a result, global counter-terrorism frameworks become more fragmented and less effective. Key pillars of the international rules-based order, including the United Nations (UN), the Financial Action Task Force (FATF), and the International Criminal Police Organization (INTERPOL), are increasingly under strain, affecting their ability to coordinate and enforce global counter-terrorism measures effectively.

Terrorists use of Asymmetry and Technological Innovation

Beyond the major global trends shaping NATO's security environment, the rapid democratization of advanced technologies is fundamentally altering the balance of technological power that is empowering non-state actors in unprecedented ways. Terrorists have never been as powerful in the technological realm as they are today, largely because advanced technologies are increasingly 'intelligent', accessible, affordable, and dual use. Today's terrorists enjoy virtually unfettered access to the advances generated by trillions of dollars in information technology investments, including social media platforms, and global IT expertise (Esvelt, 2022). Encrypted

messaging platforms and anonymization tools allow terrorist networks and lone actors to communicate, recruit, and plan operations with far greater secrecy and speed than in the past. Social media algorithms can be exploited to amplify extremist propaganda, target vulnerable audiences, and rapidly spread narratives that inspire violence across borders without the need for physical infrastructure.

In addition, the use of cryptocurrencies and online crowdfunding mechanisms enables groups to move and conceal funds outside traditional financial systems, complicating detection and disruption by authorities. Artificial intelligence tools further lower barriers by allowing terrorists to generate propaganda, deepfake videos, or multilingual content at scale, enhancing both recruitment and disinformation efforts.

Beyond the digital domain, emerging technologies also create new operational opportunities for terrorist violence. Modern terrorists have much greater access to “disruptive” technologies characterized as accessible, cheap, simple to use, transportable, and concealable (Cronin, 2020). Commercial drones can be adapted for reconnaissance or weaponized to deliver explosives, as seen in conflict zones. Advances in cyber capabilities open multiple possibilities for terrorists to conduct sabotage. Commercial drones, and 3D-printed weapons are not difficult to acquire (Esvelt, 2022). These developments demonstrate that increasingly sophisticated yet widely available technologies are readily available to terrorists.

The enhanced sophistication of terrorist organizations became increasingly evident in November 2008, when Lashkar-e-Taiba, a a terrorist organization operating primarily from Pakistani territory, attacked Mumbai over the course of 36 hours, terrorizing a city of 22 million. The ten perpetrators were able to plan, coordinate, and carry out their mission using an array of advanced devices, including global positioning system (GPS) devices and mobile phones for real-time knowledge of the urban battle space. It was a “new brand” of terrorism that practiced “urban warfare” characterized by symbolic attacks, multiple targets, and high casualties, resulting in over 170 dead, and more than 300 people injured (Liang, 2024).

At the same time, the protracted wars conducted in Mosul, Tripoli, and Kabul have underlined the need for better military doctrines in urban warfare as these are preferred battlegrounds for insurgents. The strategic and symbolic value of cities continues to attract non-state actors who use them to hijack their populations, steal resources for strategic purposes, and confront state actors asymmetrically in urban warfare. Cities are generally the preferred targets because of the population-dense targeting opportunities.

Terrorist and insurgent organizations have long pursued asymmetric warfare by exploiting technological innovations that negate the conventional advantages of state militaries. A good example is the Afghan mujahideen’s use of U.S.-supplied FIM-92

Stinger surface-to-air missiles during the Soviet–Afghan War. The introduction of these man-portable, infrared-guided missiles in the mid-1980s dramatically constrained Soviet air superiority by increasing aircraft losses and forcing changes in flight profiles, tactics, and operational tempo. From an analytical perspective, the significance of the Stinger lay not in numerical parity but in its capacity to impose disproportionate strategic and psychological costs, illustrating how access to cutting-edge military technology can enable non-state actors to neutralize a critical component of a technologically superior adversary force structure.

In the post-Cold War period, improvised explosive devices (IEDs) emerged as another paradigmatic asymmetric technology employed by terrorist and insurgent groups in Afghanistan and Iraq (Galula, 2006). IEDs exemplify technological adaptation rather than innovation: they combined commercially available components, military ordnance remnants, and basic electronics into weapons capable of inflicting sustained casualties and shaping coalition behavior (Chivers & Schmitt, 2007). Their effectiveness derived not only due to their lethality but also due to their important impact on mobility, logistics, and morale, compelling technologically advanced forces to devote extensive resources to countermeasures, route clearance, and force protection (Biddle, 2006). Scholarly analyses emphasize that IED campaigns transformed the operational environment by turning everyday infrastructure—roads, vehicles, and civilian spaces—into contested terrain, thereby eroding the conventional advantages of mechanized and networked militaries (Hoffman, 2006).

Taken together, the use of Stinger missiles and IEDs underscores a broader pattern in which terrorist and insurgent actors exploit cutting-edge or contextually disruptive technologies to conduct asymmetric attacks that reshape conflicts without achieving conventional battlefield dominance (Arquilla, J. & Ronfeldt, 2001). These technologies function as force multipliers by targeting the vulnerabilities inherent in modern military doctrines that rely on air power, mobility, and technological superiority (Petraeus & Amos, 2006). Rather than “winning” wars in a traditional sense, such asymmetric applications have often prolonged conflicts, raised political costs for intervening states, and altered strategic calculations (Kilcullen, 2009). From an academic standpoint, these cases demonstrate that the strategic value of technology in asymmetric warfare lies not in sophistication alone, but in its capacity to exploit systemic dependencies and asymmetries within modern military and political systems (Byman, 2013).

The 9/11 terrorist attack in the United States is often analyzed as an asymmetric attack on complex, networked systems **(**Hoffman, 2006). The attackers exploited vulnerabilities in civil aviation security, global transportation networks, real-time media systems, and the information environment to generate cascading effects far beyond the immediate physical damage (9/11 Commission Report, 2004). The operation relied

on modern information technologies—global communications, especially live broadcast media to amplify psychological shock and economic disruption (Rid, 2013). It also was an early demonstration of how modern societies can be strategically disrupted by asymmetric attacks on their technological and informational foundations (Arquilla & Ronfeldt, 1999). In this sense 9/11 demonstrated how attacking the connective tissue of a technologically integrated society can yield strategic effects disproportionate to the attacker's material power **(**Singer, Friedman, 2014).

By the early 2000s, a further evolution in asymmetric power had emerged, one that shifted the locus of advantage away from traditional insurgent violence toward the informational and communicative domain**.** DAESH was able to run one of the most effective misinformation and recruitment campaigns in the world with the strategic use of platforms such as Facebook, X (formerly known as Twitter), and YouTube (Liang, 2011). They were also able to use anonymizing networks and distributed platforms. This allowed terrorists to recruit followers in near real time, and project local grievances onto a global stage making it difficult for governments to disrupt content or hold actors accountable. Operating in digital spaces not governed by territorial sovereignty, DAESH also disseminated highly polished propaganda through encrypted messaging apps, and decentralized online forums, allowing its narratives to flow across borders faster than states could regulate or counter them. By blending ideological messaging with grievance narratives, selective religious symbolism, and emotional appeals to identity, belonging, and heroism, DAESH targeted disaffected young men and reframed participation in an unwinnable war as meaningful, transcendent, and urgent. Such narratives reflect distorted interpretations of religion rejected by most Muslim communities worldwide. At the same time supporter-driven amplification gave the illusion of momentum and legitimacy. Multiple sources estimate that tens of thousands of people traveled to Syria and Iraq during the peak of DAESH's territorial control—often cited at around 20,000–30,000 from over 100 countries (Cuyckens, 2022).

Terrorism Takes Place Across Multiple Domains

At the same time terrorism in the modern era transcends traditional battlefields, taking place across multiple domains—land, maritime (sea), air, space and cyber. While physical attacks will remain a threat, the digital realm is rapidly becoming the most critical arena for terrorist activity. By 2040, cyberspace and the information domain are expected to dominate, as extremist groups exploit artificial intelligence, cyber and deepfakes, to manipulate information, disrupt economies, and erode public trust. Additionally, the integration of agentic AI, autonomous systems and space-based technologies will open new fronts for sabotage.

Artificial Intelligence

Artificial intelligence is rapidly reshaping both civilian and military domains, making its security a matter of strategic significance (Janjeva, Gausen, Mercer & Sippy, 2024). Developments in AI will not only reshape the world as we know it, it will also unlock new areas of scientific discovery by supercharging the ability for scientists and engineers to discover even more advances in AI itself which will continuously remake the world in the process (Schmidt, 2025).

The rapid proliferation of generative AI systems, particularly large language models (LLMs) and agentic models, has raised growing concerns over their potential exploitation by terrorists across three principal threat domains: malicious code generation, radicalization, and weapon instruction and attack planning.

In the domain of malicious code generation, GenAI systems are increasingly being used. AI has already orchestrated the creation of numerous sophisticated malware families that demonstrate the technology's dangerous potential. Funklocker, a ransomware that uses machine learning to modify its code, has performed extortion attacks directed at governments and infrastructure across the globe, linked to hacktivist and cybercriminal activities. *Funklocker ransomware* uses living-off-the-land (LOTL) techniques by blending malicious activity with legitimate system functions to evade detection. This includes running PowerShell, taskkill, and sc commands to disable security tools, stop services, and remove recovery options (Soneye, 2025). SparkCat represents a polymorphic malware tool that uses AI obfuscation adaptation to evade antivirus detection and deploy payloads, while LameHug functions as an AI-driven worm focusing on lateral movement across networks.

LameHug is one of the first known malware that integrates LLM capabilities directly into its attack methodology (Simonovich, 2025). HexStrike-AI has weaponized neural network algorithms to generate new attack vectors autonomously. (Nova, 2025) These malware families can continuously adapt to avoid detection and perform dangerous movements across different networks, making incident response and defense increasingly difficult. In 2025, 41% of active ransomware families had integrated some form of AI modules, with 19% showing full autonomy after their launch (SQ Magazine, 2025). However current models cannot yet reliably produce novel, operational, high-stealth malware at scale. In the future, terrorists with limited technical expertise will be able to leverage these tools which will lower the bar to even more sophisticated cyberattacks.

Another significant aspect of AI-enabled threats is deepfakes and generative social engineering. Attackers use AI deepfake audios and videos to impersonate executives and deceive individuals into performing fraudulent activities. AI-powered voice phishing campaigns (vishing) have successfully tricked corporate employees by mimicking voices to authorize money transfers to attacker-controlled accounts

(Abusix, 2025). These attacks prove highly effective due to their ability to exploit human instincts like trust, ultimately bypassing verification protocols (Crowdstrike, 2025). The rapid development of deepfake technology has lowered the barrier to social engineering attacks, allowing low-skill actors to operate large-scale fraud campaigns (Esteva, 2024).

The use of deepfake technology by state actors, such as Russia's creation of a synthetic video portraying Ukrainian President Volodymyr Zelensky surrendering, highlights the potent potential of AI-driven misinformation (Chesney & Citron, 2019). Terrorist organizations could similarly exploit deepfakes to manipulate public perception, amplify fear, or disrupt political and social stability. (Westerlund, 2019) For example, they could fabricate videos of government officials issuing false directives, claiming responsibility for attacks, or spreading threatening messages to incite panic, erode trust in institutions, or provoke retaliatory actions (Vaccari & Chadwick, 2020). Combined with social media amplification, deepfakes offer terrorists a low-cost, high-impact tool for psychological operations, propaganda, and hybrid warfare, effectively weaponizing digital content without requiring physical attacks (Nguyen et al, 2019). This underscores the urgent need for robust detection technologies, media literacy, and regulatory frameworks to mitigate the malicious use of synthetic media (Kietzmann, McCarthy, & Kietzmann, 2020).

Data poisoning and model manipulation represent another critical attack vector where adversaries inject corrupted data into AI model databases, degrading system performance and altering decision-making processes while creating backdoors for exploitation. (Biggio & Roli, 2018) These attacks have targeted the healthcare industry, where AI diagnostic tools receive corrupted medical imaging and patient data, leading to misdiagnoses, delayed treatments, and erosion of trust in automated healthcare systems (Finlayson et al, 2019).

Terrorists can also acquire new funding mechanisms with the use of AI scam toolkits. There are language models designed specifically for cybercrime. These include WormGPT released in 2023 and available on the dark web, it is specifically designed for cybercrime. WormGPT allows attackers to craft Business Email Compromise messages, fake invoices with logos, and phishing emails that bypass spam filters. The growth of deepfakes has demonstrated that AI detection mechanisms are no longer sufficient countermeasures, it is important to create more sophisticated defensive approaches (Varonis Blog, 2025).

As regards weapons instruction and tactical planning, generative AI demonstrates substantial potential to enhance the capabilities of inexperienced actors through multiple ways: GenAI can deliver hyper-personalized narratives, interactive content, and tailored persuasive messaging that could transform recruitment and

indoctrination efforts. While extremist and terrorist groups have not yet widely deployed GenAI autonomously, the technology's capacity for manipulation, automated content generation, and individualized messaging poses a strategic threat that could significantly enhance terrorist organizations' ability to recruit, radicalize, and mobilize sympathizers more effectively.

The convergence of these technologies compounds the threat, as terrorists could combine AI-enabled capabilities across multiple domains to become exponentially more effective. Strategic foresight demands treating GenAI as a potential vector for terrorist activity rather than merely a technical innovation. This requires anticipatory governance, interdisciplinary evaluation frameworks, cross-sector collaboration between security practitioners and technology developers, and adaptive defense mechanisms.

Agentic AI

Agentic AI is already beginning to be used in limited but rapidly expanding forms, particularly in enterprise software, cybersecurity, and experimental defense and intelligence applications (Horowitz, 2026; Nguyen, 2026). Agentic AI in 2026 is increasingly framed as a security challenge defined by rapidly growing autonomy, opacity, and dual-use risk across both civilian and military systems (Nguyen, 2026). As AI models evolve into systems capable of independently executing multi-step tasks, they are expected to support cyber operations, intelligence analysis, logistics, and elements of operational planning, reducing the need for continuous human direction (McGuire, 2026). This shift creates what analysts describe as a “shadow autonomy” problem, where AI agents operate in ways that are difficult to fully observe or verify, while adversaries may already be using similar systems to accelerate intrusion and attack workflows (Nguyen, 2026).

These risks are compounded by “shadow identity,” where synthetic or AI-generated actors blur the distinction between legitimate and hostile users, and “shadow code,” where large volumes of AI-generated software enter critical infrastructure without clear visibility into vulnerabilities or provenance (Nguyen, 2026). Together, these dynamics reduce trust in automated systems even as reliance on them expands across defense and industry, making observability and verification central security concerns (Nguyen, 2026).

In response, NATO is expected to increasingly integrate agentic AI into its command-and-control and multi-domain operations, using autonomous systems to support real-time intelligence fusion, threat detection, cyber defense, and logistics coordination across allied forces (Brandt, 2026). Such systems could enable faster decision cycles by aggregating data from multiple member states and generating adaptive operational recommendations, while also coordinating unmanned assets in

air and maritime environments (Brandt, 2026). However, this reliance on agentic systems would also heighten NATO's exposure to the same transparency and attribution challenges, making secure AI governance and interoperable standards across allies a critical priority (Brandt, 2026).

At the same time, terrorist and extremist groups could exploit agentic AI to automate elements of cyber intrusion, target selection, and propaganda dissemination at a scale and speed that would be difficult for human operators to match (McGuire, 2026; Nguyen, 2026). They could also use autonomous AI agents to coordinate low-cost, distributed attacks or to identify and exploit vulnerabilities in public infrastructure and digital systems with minimal direct oversight (Nguyen, 2026).

5G

The deployment of fifth-generation (5G) communications infrastructure has introduced a new set of strategic challenges for the United States and NATO, extending beyond traditional state-based competition to include non-state and terrorist actors. (Li & Zhang, 2021) From an academic perspective, 5G represents not merely an incremental improvement in bandwidth, but a foundational shift toward software-defined, virtualized, and highly decentralized networks that underpin military command-and-control, critical infrastructure, and civilian life (Rinaldi, McDaniel, & Van Meter, 2020).

While much scholarly and policy attention has focused on state actors exploiting 5G through espionage, supply-chain influence, or strategic dependency, the same architectural features—network slicing, edge computing, and massive device connectivity—also expand the attack surface available to asymmetric actors (Xu, He & Zhang, 2021). Terrorist groups, historically adept at exploiting civilian technologies for disruptive effect, are therefore positioned to benefit indirectly from the diffusion of 5G-enabled systems, particularly where civilian and military networks intersect or where governance and security standards are unevenly enforced (Nye, 2011).

For terrorist organizations, the challenge posed by 5G is less about direct technological mastery and more about opportunistic exploitation of systemic complexity and dependency (Borrion, Shand, & Macintosh, 2020). 5G-enabled environments support dense ecosystems of Internet of Things (IoT) devices, autonomous systems, and real-time data flows, all of which can become vectors for disruption, surveillance, or influence operations if inadequately secured (Chen, Ma, Li & Wu, & Zhang, 2018). From a NATO perspective, this blurs the distinction between cyber, physical, and informational domains, as attacks need not compromise core network infrastructure to achieve strategic effects; targeting peripheral devices, edge nodes, or civilian-dependent services may suffice to generate disruption, fear, or cascading failures (CCDCOE. 2021). Consequently, 5G intensifies the asymmetric

advantage traditionally enjoyed by terrorist actors by embedding critical societal functions within technologically complex systems that are difficult to defend comprehensively (Kshetri, 2021). This development underscores the need for NATO and allied states to conceptualize 5G not only as a geopolitical or industrial-security issue, but as a multi-domain vulnerability in which state and non-state threats converge (ENISA, 2020).

Terrorist attacks explicitly targeting 5G networks are rare, but there have been incidents where extremist violence and sabotage has impacted 5G infrastructure (Smith & Jones, 2020). During 2019–2021, telecommunications masts in the United States and in several European countries were vandalized or set on fire, sometimes framed by perpetrators as resistance to perceived technological or governmental threats; while many of these acts were driven by conspiracy movements rather than formally designated terrorist organizations, security services assessed some cases through a counterterrorism lens because of their ideological motivation, intent to intimidate, and targeting of critical infrastructure (Europol, 2021).

In conflict and insurgency contexts, armed groups have also attacked cellular towers and mobile infrastructure, including early 5G-capable sites, to disrupt communications, undermine state authority, and generate psychological impact—continuing a long-standing pattern of targeting telecom networks (Cockayne & Lupel, 2018). Additionally, religiously motivated extremist and far-right extremist propaganda has periodically referenced next-generation communications infrastructure as a symbol of state control or societal corruption, encouraging supporters to view such systems as legitimate targets (Bertram & O'Hara, 2020). Collectively, these cases suggest that while terrorists have not yet demonstrated sophisticated cyber exploitation of 5G core networks, physical attacks, intimidation, and ideologically framed sabotage of 5G-related infrastructure already fit within established terrorist repertoires, reinforcing concerns about the vulnerability of highly networked civilian systems (Rinaldi et al. 2020).

Smart Cities and the Proliferation of the Internet of Things (IoT)

Recent studies highlight the growing security risks posed by the large-scale exploitation of Internet of Things (IoT) devices. As cities evolve into "smart" urban systems—characterized by pervasive sensors, interconnected platforms, and data-driven governance—these same features create new opportunities for exploitation. The proliferation of IoT has fundamentally transformed the cyber threat landscape by embedding vast numbers of networked devices throughout urban space.

The risks associated with IoT insecurity are further amplified by the integration of connected devices into critical infrastructure, including smart cities, utilities, and healthcare systems, where cyber vulnerabilities can have direct physical

consequences (Patel, 2025). For example, the compromise of smart traffic light systems can increase the likelihood of traffic accidents, while attacks on water quality sensors pose risks to public health through potential contamination.

Compromised IoT devices can be repurposed into botnets for large-scale cyber operations or used to disseminate propaganda that amplifies perceptions of control and reach (Rose, Eldridge & Chapin, 2015). As smart homes, traffic management systems, environmental sensors, public safety cameras, and industrial control systems proliferate, they collectively expand the attack surface far beyond traditional IT networks (Roman, Zhou & Lopez, 2013). In this sense, smart cities are not only potential targets but also enabling environments, where interconnected civilian technologies can be weaponized to achieve strategic effects without crossing conventional thresholds of armed attack (Zanella et al, 2014).

Many of these devices are minimally secured, lack regular patching mechanisms, and are deployed at scale with limited oversight (Sicari et al, 2015). Consequently, IoT infrastructure has shifted from a convenience-driven innovation to a significant source of systemic vulnerability (Conti et al, 2018). Malicious actors, including extremist groups, can exploit smart-city IoT through ransomware or denial-of-service attacks to degrade public services, undermine trust in authorities, and generate broader political impact (Borrion, Shand & Macintosh, 2020).

The Mirai botnet of 2016 exemplifies the first generation of IoT-driven cyber threats (Woolf, 2016). Mirai exploited default credentials on consumer-grade devices such as routers, IP cameras, and DVRs to form botnets capable of massive distributed denial-of-service (DDoS) attacks. High-profile incidents, including the Dyn DNS attack, demonstrated how even unsophisticated malware could cause widespread disruption to critical online infrastructure, affecting services like X (formerly known as Twitter), Netflix, and PayPal. Mirai's significance lay not in technical sophistication but in amplifying systemic vulnerability through scale, transforming everyday consumer devices into tools of asymmetric disruption (Woolf, 2016). This event catalyzed a broader understanding of the potential for IoT devices to become vectors for both kinetic-style impact in the digital realm and societal disruption.

By 2025, the threat landscape had evolved with malware such as BadBox, which represents a more strategically sophisticated exploitation of IoT systems. A 2025 report by Asimily, an IoT security analytics firm, documents how the BadBox 2.0 botnet compromised more than 100 million IoT devices worldwide, including smart televisions, in-car entertainment systems, and digital photo frames (Jones, 2025). The botnet leveraged pre-installed malware, malicious application downloads, and command-and-control channels to create a globally distributed network used for click fraud, device hijacking, proxy service abuse, and distributed denial-of-service (DDoS)

attacks. Similarly, research reported by *Cybersecurity Dive* indicates that the Iranian-linked Eleven11bot campaign infected approximately 86,000 IoT devices—primarily security cameras and network video recorders—which were subsequently weaponized to launch DDoS attacks against telecommunications and gaming companies in the United States (Jones, 2025). BadBox leveraged supply-chain compromises and preinstalled firmware infections to infiltrate Android-based devices worldwide, creating persistent and stealthy botnets (Trend Micro, 2022). Unlike Mirai, BadBox-enabled networks were multifunctional: they supported DDoS activity but also facilitated financial cybercrime operations such as click fraud, proxy networks, and credential theft (Check Point Research, 2021). The combination of stealth, global reach, and monetization reflects a shift from temporary disruption toward sustained, multifunctional exploitation, illustrating the increasing strategic utility of IoT malware in both criminal and hybrid threat contexts (Antonakakis, Bailey, 2017).

The trajectory of IoT malware suggests that future variants of both Mirai-style and BadBox-style threats may become even more adaptive, stealthy, and autonomous (Symantec Threat Intelligence, 2022). Emerging techniques could include machine-learning–driven propagation, zero-day firmware exploitation, encrypted and polymorphic command-and-control traffic, and blending of malicious activity with normal IoT communications (IBM X-Force Research, 2023). Such advances would complicate attribution and mitigation efforts, enabling attackers—including criminal syndicates, state actors, or ideologically motivated groups—to manipulate both digital and physical infrastructures with systemic, hard-to-detect impact (ENISA, 2021). The convergence of ubiquity, automation, and stealth thus underscores the asymmetric advantage IoT exploitation can confer to technologically resource-limited actors (Conti et al, 2018).

The evolution from Mirai to BadBox highlights the growing intersection of technological ubiquity, systemic vulnerability, and asymmetric threat (Lin & Berg, 2020). Whereas Mirai exposed the dangers of scale and poor credential hygiene, BadBox demonstrates the risks posed by supply-chain compromise, persistent infections, and multifunctional botnets (Chen, Liu & Zhang, 2022). Looking ahead, addressing the evolving IoT threat landscape requires a combination of robust device security standards, proactive supply-chain monitoring, coordinated incident response, and regulatory frameworks that incentivize secure design (NIST, 2021). Failure to adapt could allow future IoT malware to produce not only temporary disruption but sustained, strategic, and financially or politically significant effects, making it a central concern for both cybersecurity professionals and policymakers (Kshetri, 2021).

The growing intersection of technological ubiquity are already being used in the Russia-Ukraine War interconnected networks and systems to attack power grids, public services, and communications (Krebs, 2025). Cyber campaigns linked to the

conflict in Ukraine have demonstrated how adversaries can exploit interconnected digital and physical systems to disrupt power grids, public services, and communications networks (Abraham, Houmb & Erdodi). Collectively, these developments underscore the need to reconceptualize cybersecurity as a core component of national security strategies and highlight the importance of strengthening IoT resilience, enhancing international collaboration, and establishing norms to govern behavior in cyberspace (Patel, 2025).

Looking forward, advances in AI and deepfakes will enable more convincing disinformation and social-engineering campaigns that can spoof official alerts or delay responses, while cheap drones and autonomous platforms integrated into city infrastructure create new tactical delivery and reconnaissance options for non-state actors.

Real-world incidents — from malware that disrupted municipal heating and utilities to documented efforts by violent actors to use digital platforms for coordination — demonstrate these pathways are not hypothetical and will intensify as cities digitize without commensurate cyber resilience. Smart-city benefits (efficiency, safety, service continuity) can be turned against populations unless cities and national authorities prioritize hardened architectures, segmentation, secure supply chains, continual threat-monitoring, and public-private information-sharing to deny extremists easy, deniable avenues into urban systems (ENISA, 2025).

Subsea Data Cables

As global reliance on digital connectivity deepens, the physical vulnerability of subsea data cables presents another increasingly attractive target for terrorist groups seeking to generate widespread disruption with relatively limited operational investment. Subsea communication cables constitute a foundational component of the global information and communications technology (ICT) ecosystem, carrying more than 95 per cent of worldwide internet, voice, and data traffic through approximately 1.3 million kilometers of cable laid across the globe (Kavanagh, 2023). The strategic significance—and inherent fragility—of this infrastructure has been underscored in recent months by events in the Bab al Mandab Strait, a critical maritime chokepoint at the southern entrance to the Red Sea. In February 2024, reports indicated that at least three major subsea fibre-optic cables—Asia Africa Europe 1 (AAE-1), Europe India Gateway (EIG), and the Seacom/TGN Gulf system—were severed, resulting in disruptions to approximately 25 per cent of internet traffic flowing between Asia, Africa, and Europe (PBS, 2025). These incidents illustrate how attacks on subsea cable infrastructure could be leveraged by terrorist actors to amplify economic, informational, and societal disruption on a transnational scale.

While the Houthi movement, which controls large parts of northern Yemen, has denied direct responsibility for cutting the cables in the Bab al Mandab region, its sustained attacks on commercial shipping have markedly elevated the risk to undersea networks operating in close proximity to active hostilities (Naval Technology, 2024). Analysts note that even in the absence of intentional sabotage, such attacks can have cascading effects. In the case of the bulk carrier *MV Rubymar*, which was struck by Houthi missiles and subsequently abandoned while drifting above a known cable zone, investigators suggest that the vessel's anchor may have dragged across the seabed in relatively shallow waters (approximately 100–300 meters), severing multiple cables in the process (Al Arabiya, 2024). These risks are further compounded in conflict-prone maritime corridors, where militant activity increases the likelihood of both deliberate and incidental damage to subsea infrastructure.

This episode exposes the latent fragility of undersea cable systems in narrow maritime chokepoints. In the Bab al Mandab Strait—through which an estimated 90 per cent of Europe–Asia fiber-optic traffic transits—the convergence of geopolitical conflict and physical vulnerability transforms what is typically a commercial maritime risk into a matter of global strategic concern (Naval Technology, 2024).

Comparable dynamics have emerged in the Baltic Sea, where a series of high-profile incidents has further underscored the security implications of undersea infrastructure disruption. In November 2024, two fiber-optic cables linking Finland to Germany and Lithuania to Sweden were severed, with investigators publicly treating the damage as likely sabotage. Subsequent damage to power and telecommunications cables between Finland and Estonia triggered criminal investigations and charges against the crew of a tanker suspected of dragging its anchor across the seabed (Ahlander, Lehto, Systos, 2024). These incidents prompted rapid repair operations, heightened political alarm across Northern Europe, and led NATO and EU actors to reframe undersea infrastructure protection as a frontline security issue rather than solely a commercial responsibility.

Taken together, these episodes illustrate two critical realities of contemporary digital connectivity. First, the global internet remains physically fragile: a limited number of cable cuts or the loss of a single power link can significantly degrade network capacity, increase latency, and impair state and civilian communications across vast regions, even where redundancy exists. Second, whether through intentional sabotage or reckless activity that is operationally indistinguishable from it, attacks on civil undersea infrastructure enable coercive effects characteristic of hybrid warfare. For terrorist and militant actors, such vulnerabilities offer an asymmetric means of generating strategic disruption disproportionate to the resources required.

These episodes illustrate two interrelated realities of modern connectivity. First, the internet remains physically fragile: a small number of cable cuts or even a single power-supply failure can degrade capacity, increase latency, and disrupt state and civilian communications across wide regions, even in systems designed with redundancy (Starosielski, 2015). Second, intentional sabotage—or reckless activity that is operationally indistinguishable from it—can transform civilian infrastructure into a tool of coercion and hybrid warfare (Rid, 2020). The Baltic incidents, in particular, demonstrate how ambiguous attribution and “shadow fleet” behavior can generate strategic effects that far outweigh the immediate technical damage (Brunsden & Peel, 2023). Together, these dynamics underscore that telecommunications resilience is no longer merely a matter of commercial continuity but a core national-security concern and an important international security priority that needs to be tackled (NATO 2023).

Addressing this vulnerability requires a phased response that combines immediate safeguards with longer-term structural reform. In the near term, priorities include faster detection and repair through expanded cable-repair fleets and pre-positioned spare components, along with transparent international incident-reporting mechanisms (ITU, 2021). Emergency traffic-rerouting agreements between operators and states would further reduce the operational impact of disruptions (Clark, Lehr, Bauer, 2019). At the same time, protecting cable routes demands enhanced maritime domain awareness, including surface and subsea sensors, advanced AIS and ship-movement analysis, and intelligence sharing among allies (NATO Maritime Command, 2022). These measures should be reinforced by legal steps to formally designate subsea cables as critical infrastructure and to criminalize deliberate interference (UNGA, 1982, ENISA 2022).

Looking toward 2040, resilience will depend on reducing systemic dependence on single points of failure. Governments and industry should invest in more distributed network topologies, including diverse routing options and terrestrial backstops, alongside hardened cable design and deeper burial where feasible. Advances in autonomous inspection and repair drones can lower response times and risks, while strengthened public–private frameworks can ensure operators receive timely state protection during periods of heightened threat. Ultimately, technical and legal measures must be complemented by multilateral norms and treaties—establishing rules of engagement for undersea infrastructure and cooperative rapid-response mechanisms—to deter actors who calculate that cable disruption can yield political leverage. Taken together, these technical, legal, and diplomatic efforts are mutually reinforcing; neglecting anyone increases the likelihood that future conflicts will weaponize the very networks that bind contemporary societies together (Thevenin, 2025).

LEO satellites

Low Earth Orbit (LEO) satellites and underground subsea cables constitute the nervous system of the global communications network, they carry more than 99 percent of global dataflows within and across continents through fiber-optic cables beneath the waves, providing critical services such as navigation, surveillance, and internet connectivity (Kirkman, 2024). These assets are especially vulnerable to interference, espionage, and sabotage. As emerging markets increasingly participate in building and deploying these systems, NATO must assist in setting standards for cybersecurity, satellite resilience, and the protection of physical and digital infrastructure. Securing these channels ensures that data flows remain trustworthy and that command and control systems critical to defense remain uncompromised by adversarial influence or criminal exploitation.

Although there are no verified instances of terrorists physically attacking satellites in Low Earth Orbit (LEO), non-state actors have previously exploited space infrastructure in ways that signal emerging threats to orbital systems. The most prominent case occurred in 2007 when the Liberation Tigers of Tamil Eelam (LTTE), designated as a terrorist group, hijacked a vacant Ku-band transponder on an Intelsat communications satellite to broadcast propaganda for more than a year before the signal was shut down by the operator (Intelsat Ltd) in 2007 (East Asia Forum, 2021; Satellite Today, 2007). This incident did not involve a LEO satellite or physical destruction but demonstrated that militant groups can compromise space communications to achieve strategic messaging. There are also documented episodes of signal jamming and hijacking by non-state groups and movements, such as disruption of satellite broadcasts in China during the early 2000s (Space and Defense Trends Analysis, 2025), further illustrating how space assets can be manipulated by irregular actors.

As satellites become more numerous—especially in LEO where commercial constellations proliferate—the risk landscape is shifting from purely kinetic threats to cyber-physical vulnerabilities. Satellite systems depend on ground control, uplink/downlink communications, and software interfaces that can be targeted by adversaries, including signal interference, denial of service, or command spoofing (PwC, 2025; Ballard et al., 2025). These modes of attack are more accessible to non-state actors than direct kinetic engagement and could allow a terrorist group to degrade critical services such as communications, navigation, or internet connectivity without having to reach orbit. The increasing integration of space infrastructure into terrestrial critical systems—combined with lowered barriers to cyber and electronic exploitation—means that future attacks on satellites or their networks by terrorists, while still technically demanding, are conceptually plausible and require proactive mitigation (Chatham House, 2016; Space and Defense Trends Analysis, 2025).

Terrorist and extremist groups are already exploiting the rapid proliferation of LowEarthOrbit (LEO) satellite services in ways that amplify their operational reach without requiring state sponsorship: commercially available satellite-internet terminals and imagery give them resilient communications and real-time reconnaissance in areas where terrestrial networks are degraded or deliberately shut down. These capabilities let groups coordinate dispersed cells, maintain encrypted links to command nodes, monitor troop movements or convoy routes from open-source satellite imagery, and sustain propaganda and recruitment campaigns from otherwise isolated safe havens — all while reducing their dependence on vulnerable terrestrial infrastructure.

At the same time, the LEO ecosystem presents technical attack surfaces (e.g., jamming, spoofing, cyber intrusions against ground stations or network operations) that adversaries and criminal intermediaries can seek to exploit or rent out, and service outages or single-vendor failures can create brittle dependencies that armed groups may seek to weaponize tactically. Reports from the Sahel to Southeast Asia show this is not theoretical: commercial satellite kits have been seized in conflict zones and used by militant groups, and cybersecurity assessments highlight concrete vulnerabilities across LEO satcom architectures that criminal and hostile actors could leverage (Le Monde, 2025).

Ultimately, protecting the technological arteries of the 21st century is as vital as defending borders or airspace. NATO must adopt a proactive strategy to ensure that advances in LEO satellites, underground cables, smart city and AI technologies continue to be engineered in and among nations committed to stability, transparency, and the rule of law. Through partnerships, information sharing, and investment in capacity-building, NATO can help emerging markets develop these systems securely by creating a global ecosystem resistant to infiltration by extremist or criminal actors. In doing so, the Alliance will not only defend its member states but also uphold the integrity of the interconnected world on which global security increasingly depends.

Drones

We are also witnessing worldwide a convergence between battlefield drone innovation and modern terrorist tactics, driven largely by lessons learned from the wars in the Russia–Ukraine conflict, the US–Israeli confrontation with Iran, and ongoing conflicts in Africa and the Middle East (Stockhammer, 2026). We are increasingly seeing extremist groups adapting military-style drone practices for asymmetric attacks against civilian targets (Stockhammer, 2026). Cheap commercial drones can be easily modified into airborne weapons, while first-person-view (FPV) drones—refined on the battlefields of Ukraine—have demonstrated how small, maneuverable systems can evade conventional defenses and deliver explosives with precision (McGuire, 2026).

These developments have heightened fears across Europe that DAESH-inspired groups or criminal proxy networks might employ drones in attacks on crowded public spaces. Security agencies worldwide are preparing for multiple terrorist attack scenarios targeting concerts, sports tournaments, airports, shipping infrastructure, and internationally visible cultural events, all of which represent particularly vulnerable “soft targets” (Nguyen, 2026).

Drone warfare is fundamentally reshaping the security architecture of the Sahel by altering the balance between state military forces and non-state armed groups. The increasing accessibility of commercial unmanned aerial vehicles (UAVs), particularly first-person-view (FPV) drones, has enabled insurgent and terrorist organizations to adopt low-cost but highly effective aerial capabilities previously associated with conventional military powers (Okpaleke et al., 2023).

In recent years, terrorist organizations operating across Mali, Burkina Faso, Niger, and northern Nigeria have increasingly incorporated drones into surveillance, reconnaissance, propaganda dissemination, and offensive operations. The most prominent groups employing such technologies include Jama’at Nusrat al-Islam wal-Muslimin (JNIM), Islamic State West Africa Province (ISWAP), Islamic State Sahel Province (ISSP), and factions associated with Boko Haram (Al Jazeera, 2026; Sallama, 2026).

JNIM, affiliated with Al-Qaeda, has emerged as one of the most technologically adaptive militant groups in the central Sahel. Since 2023, the organisation has increasingly deployed modified commercial drones carrying improvised explosive devices (IEDs) and mortar rounds in coordinated assaults against military installations in Mali and Burkina Faso (ISS Africa, 2025). Similarly, ISWAP and Boko Haram factions operating within the Lake Chad Basin and northeastern Nigeria have adopted armed drone tactics against military bases in Borno and Yobe States (Reuters, 2025).

The proliferation of FPV drones represents a significant tactical evolution because such systems provide insurgents with enhanced situational awareness, precision targeting, and psychological impact at relatively low financial cost. These drones are often commercially available Chinese-manufactured systems retrofitted for military purposes, thereby circumventing traditional arms control mechanisms (Koné and Koné, 2025).

The Sahel’s vast ungoverned spaces further facilitate the operational effectiveness of drone warfare. Regions such as the Mali–Burkina Faso–Niger tri-border area, the Sambisa Forest, and the Lake Chad Basin provide ideal environments for insurgent mobility, concealment, and drone deployment (Okpaleke et al., 2023). Consequently, drone warfare has intensified asymmetrical conflict dynamics by

reducing insurgents' dependence on direct battlefield confrontation while increasing their capacity to conduct remote attacks and intelligence gathering.

A parallel but distinct dynamic is observable in Türkiye, where the PKK has adapted drone tactics following methods previously employed by DAESH. Framed as a "learning organization," the PKK has incorporated drones into its attacks, prompting a focused counter-response from Ankara. In turn, Türkiye has systematically increased its investments in anti-drone systems, demonstrating how a state can adapt to the dynamic structure of the asymmetric drone threat by placing emphasis on hybrid and counter-drone solutions (Özgen & Kurt, 2025).

The appeal of drones to militant organizations is clear: they are inexpensive, difficult to detect, easy to acquire and modify, and capable of bypassing traditional air-defense systems. More recently, terrorists have also experimented with fiber-optic guided drones, which are resistant to electronic jamming and interception (Nguyen, 2026). Beyond their tactical advantages, drones also carry significant psychological value. Footage captured by onboard cameras can be rapidly disseminated online, transforming attacks into propaganda spectacles designed to amplify fear far beyond the immediate site of violence.

Security experts highlight the growing use of AI-assisted targeting and propaganda, as well as "swarm" tactics that combine drones with missiles or coordinated multi-vector assaults. Transitioning toward a theory of warfare centered on swarm weapons requires moving beyond the traditional emphasis on sheer mass. Rather than relying solely on concentrated force, swarms of drones apply the principle of maneuver in a new way: by dispersing across the battlefield and striking hundreds of vulnerable points within an enemy system simultaneously. This ability to overwhelm defenses through coordinated, multi-directional attacks fundamentally alters how military power can be projected and how adversaries must think about defense (McGuire, 2026).

China and the United States are both advancing toward distributed, AI-enabled unmanned warfare, but through distinct strategic pathways. China's approach integrates autonomous surface swarms such as the L30 system, AI-driven coordination frameworks like the Atlas architecture, and platform enablers such as the Type 076 *Sichuan* drone carrier and airborne mothership concepts like "Jiutian," all designed to link sea, air, and potentially underwater domains into a unified swarm network (Segal, 2026). The United States, in contrast, is planning to field at least 1,000 unmanned aircraft to accompany its F-35 and Next Generation Air Dominance platforms. These collaborative combat aircraft (CCAs), along with autonomous naval systems such as the Ghost Fleet Overlord programme and broader unmanned surface and undersea fleets, are forming part of a "hybrid" manned–unmanned force structure

coordinated through advanced battle networks (Brandt, 2026). In parallel, NATO is exploring interoperable autonomous systems and multi-domain command architectures aimed at ensuring allied forces can integrate drone swarms, maritime unmanned vessels, and AI-enabled decision systems across member states, reflecting a shared but uneven transition toward network-centric, distributed warfare (Brandt, 2026).

In the future, drones will become both critical security threats and indispensable operational enablers. As they become increasingly embedded in the protection of critical infrastructure and in public and commercial services, it will be essential for NATO to develop robust Unified Threat Management (UTM) systems and reliable counter-drone capabilities. These will need to range from passive monitoring to active neutralization, supported by clear tactics, techniques, and procedures, as well as well-defined rules of engagement to ensure safety and stability across key defence domains (Nguyen, 2026).

Engineered Terrorism - the Birth of Synthetic Asymmetry

Modern warfare has shifted dramatically with profound changes within the global technological landscape. New and emerging technologies are making conflicts more asymmetric, technologically complex, and harder to identify and resolve, blurring lines between combatants and civilians, states and non-state actors while also challenging traditional military doctrines. (Krepinevich, 1994) These dynamics point to the emergence of what can be described as synthetic asymmetry—a qualitative leap beyond the traditional forms of asymmetric warfare historically employed by terrorist organizations (Hoffman, 2007).

Whereas earlier asymmetry relied on simple weapons, terrain advantages, or improvisation, contemporary asymmetry is increasingly embedded within complex technological systems that scale rapidly and independently and operate across domains(Arquilla & Ronfeldt, 2001). Recent experience demonstrates that virtually everything can be weaponized: information ecosystems manipulated through AI-driven influence campaigns, supply chains exploited via digital dependencies, IoT devices repurposed into botnets, subsea data cables targeted to block the internet and space assets hijacked to maintain communication (Rid, 2020).

Contemporary conflict increasingly reflects what Venable terms synthetic asymmetry*:* a form of engineered advantage arising not from a single technology, but from the deliberate convergence of multiple civilian, commercial, and military domains. (Venable, 2022) Synthetic asymmetry is constructed through the interoperability of digital, informational, and infrastructural systems, allowing weaker actors to generate nonlinear effects that far exceed their material capabilities (Nye, 2011). In the Ukraine–Russia war, Ukraine offset Russia’s conventional superiority by integrating commercial

satellite communications, open-source intelligence, AI-assisted targeting, civilian drones, and cryptocurrency-enabled funding into a coherent operational system (Watling and Reynolds, 2022; Kofman et al., 2023; Venable, 2024). Similarly, the Houthis' use of low-cost drones and GPS-guided cruise missiles to strike Saudi oil infrastructure demonstrates how commercially available components, when combined with basic digital navigation and targeting, can extend the reach of non-state actors well beyond traditional guerrilla constraints (Knights, 2020). In both cases, widely accessible technologies enabled weaker actors to generate disproportionate operational and strategic effects.

A second pillar of synthetic asymmetry lies in the weaponization of information ecosystems, particularly through AI-enabled influence operations that collapse the boundary between civil society and conflict. Since at least 2016, Russia has employed troll farms, bot networks, and platform algorithms to manipulate political discourse in the United States and Europe, increasingly augmenting these efforts with generative AI and deepfake media to scale persuasion at minimal cost (Howard et al., 2018; DiResta, 2023). Western governments have also faced scrutiny over the use of AI-driven influence tools, strategic communications, and algorithmic content amplification in both domestic and foreign information environments. China has adopted similar techniques through AI-assisted content farms and synthetic online personas to shape narratives on Taiwan, COVID-19, and Xinjiang across languages and platforms (Han, 2022; ASPI, 2023). Such operations exemplify cognitive-domain asymmetry: they enable relatively small or covert actors to polarize societies, erode institutional trust, and pursue political objectives without kinetic force (Venable, 2024). The disproportionate ratio of effort to impact—where automated systems amplify influence far beyond human capacity—marks a defining characteristic of synthetic asymmetry.

A third manifestation of asymmetry is also embedded in digital supply-chain dependencies, where exploitation of a single node can cascade across global systems. where tightly coupled systems create high-leverage points for disruption. The SolarWinds intrusion demonstrated how compromising a single trusted software update could cascade into thousands of affected networks across governments and corporations (CrowdStrike, 2020; U.S. Senate, 2021), while the Log4j vulnerability revealed near-universal exposure stemming from a ubiquitous open-source component (CISA, 2021). Beyond cyberspace, China's dominance in rare-earth processing illustrates a digitally managed supply-chain asymmetry that enables coercive leverage over advanced manufacturing and defense sectors (Humphries, 2019; Gholz, 2021). All these systems when studied individually present manageable vulnerabilities, however when combined, produce systemic fragility. Taken together, these examples demonstrate that synthetic asymmetry is not accidental but engineered. In this environment, asymmetry is no longer improvised at the margins; it is manufactured through access to global technological infrastructures**.** If these

infrastructures are shaped without robust security norms, accountability mechanisms, and counter-extremism considerations, they risk empowering not only rival states but also non-state actors capable of synthesizing technological domains into strategic power by exploiting the connective tissue of the modern world for disruptive and coercive ends while simultaneously challenging existing doctrines of deterrence, governance, and international law.

Private technology companies—and the tech industry as a whole—will play a crucial role in shaping global competition, irregular warfare, and the development of resilient cybersecurity capabilities, both today and in the years ahead. Without effectively integrating these private actors into its security framework, NATO's ability to contain violent non-state threats and maintain its position as the world's most secure and technologically advanced defense alliance will be significantly weakened.

Towards a New Tech Axis of Security (Nations, Industries and Individuals)

For decades, the United States has held unrivalled technological pre-eminence, conferring both material advantage and influence over the global digital order. American firms have constructed and managed strategically significant digital infrastructure—from cloud architectures and data centers to software ecosystems and social platforms—and now derive substantial revenue from international markets, sustaining continuous reinvestment in innovation and workforce development (West, 2021). Yet this hegemony carries dual consequences. While enabling global connectivity and economic growth, U.S. digital platforms, particularly social media conglomerates, have at times facilitated misinformation, radicalization, and authoritarian surveillance, revealing the tension between technological innovation and destabilizing externalities (Gorwa et al., 2020). American technological leadership thus embodies both strategic power and ethical responsibility, requiring alignment of innovation with democratic values, transparent governance, and global stewardship.

U.S. technological dominance is not solely economic; it underwrites NATO's strategic advantage in secure communications, intelligence coordination, and digitally enabled operations. Advanced cyber defense architectures, secure cloud platforms, and AI-driven threat analysis rely heavily on American industrial capacity, making technological pre-eminence a pillar of transatlantic security (NATO, 2022). However, this dominance faces mounting competition. China's investment in quantum computing, 5G networks, AI, and infrastructure in the Global South through initiatives such as the Digital Silk Road demonstrates a concerted effort to establish alternative technological standards and governance models, challenging Western norms and exerting geopolitical influence (Segal, 2020). This intensifying rivalry underscores the need for NATO and its members to innovate continually to maintain digital superiority.

Maintaining this edge is not merely competitive but essential for global security. As computing infrastructures diversify, vulnerabilities—particularly in systems influenced by authoritarian actors—proliferate, creating opportunities for exploitation by non-state actors adept at leveraging digital asymmetries. Extremist or malign actors could weaponize emerging technologies, infiltrate critical networks, or manipulate autonomous systems, destabilizing the broader security environment (Venable, 2024). NATO's response must therefore fuse innovation, governance, and ethical foresight: sustaining U.S. technological leadership while coordinating Alliance-wide investment in indigenous capabilities, cyber resilience, and proactive vulnerability mitigation. Only through such collective adaptation can NATO preserve strategic advantage and safeguard the integrity of the global digital ecosystem against both state and sub-state threats.

NATO and the Integration of Tech Titans

Frontier AI companies, defence technology firms, and hyperscale cloud providers will increasingly need to collaborate closely with NATO and its member states to balance three competing imperatives: democratic accountability, operational security, and geopolitical competition (Horowitz, 2026; Brandt, 2026). As agentic and foundation AI systems become embedded in intelligence, logistics, and command-and-control functions, NATO will depend on industry partners not only for cutting-edge capabilities but also for secure infrastructure, model assurance, and resilient cloud environments capable of withstanding adversary disruption (Nguyen, 2026).

In recent years, NATO has increasingly recognized the necessity of engaging with leading technology companies to maintain strategic advantage in the domains of artificial intelligence, space operations, robotics, and advanced materials. This shift reflects the Alliance's acknowledgment that national security is no longer solely the purview of states; private-sector innovation, led by figures such as Elon Musk, Jeff Bezos, Mark Zuckerberg, and Sam Altman, now underpins critical capabilities that directly influence NATO's operational readiness. Rather than attempting to exert direct control over individual actors, NATO has pursued a strategy of structured engagement, investment, and partnership to align commercial incentives with collective security objectives.

The growing concentration of power and influence in the hands of a small number of "Tech Titans"—the CEOs, founders, and major shareholders of leading technology companies—represents a structural shift in the global security environment, particularly for alliances like NATO (Farrell & Newman, 2019). These individuals and their companies increasingly control the digital backbone of the world, from cloud computing, AI platforms, and satellite networks to 5G infrastructure and critical data flows (Zuboff, 2019). Such concentration of power creates both

opportunities and vulnerabilities. On the one hand, collaboration with technologically advanced private actors can significantly enhance NATO's operational capabilities, accelerate innovation in defense and intelligence, and facilitate resilience across multiple domains, including cyber, space, and communications (NATO, 2021). On the other hand, reliance on a narrow set of corporate actors can create systemic dependencies, where the geopolitical or commercial decisions of a few individuals could inadvertently—or deliberately—affect national security, critical infrastructure, or the resilience of democratic states (Tooze, 2021).

For NATO and its member states, the challenge lies in aligning the strategic interests of these private actors with collective defense and democratic norms. NATO must ensure that these global technology titans including: Elon Musk, Jeff Bezos, Mark Zuckerberg, and Sam Altman are willing to support multilateralism and global stability. Tech titans and their companies are not traditional actors in global security, but their platforms, infrastructure, and innovations in AI, satellites, cloud computing, and logistics have become critical to the functioning of societies and defense ecosystems (Kania, 2020).

Unlike nation-states, Tech Titans operate primarily on profit incentives, market growth, and global influence, which may not automatically coincide with alliance security priorities (Nye, 2011). The risk is compounded by global competition: adversarial states, particularly China, have demonstrated the capacity to cultivate and integrate corporate ecosystems that operate in ways that advance state objectives, often without regard for liberal democratic values (Segal, 2018). If Tech Titans are enticed by markets or partnerships in countries with authoritarian governance or weak security standards, critical technologies and infrastructure could shift outside NATO-aligned control, undermining both operational security and normative influence in emerging digital ecosystems (European Commission, 2020).

Ensuring that Tech Titans remain committed to NATO and democratic values will require a multi-faceted approach (NATO, 2021; Nye, 2011). First, NATO should foster high-level, structured engagement channels that allow these leaders to participate in shaping frameworks for technology resilience and security. This can include advisory councils, private roundtables, and joint research initiatives where corporate innovations are aligned with NATO's strategic imperatives, such as secure satellite communications, resilient AI systems, and cyber defense standards. (NATO, 2022; European Commission, 2020). These policy frameworks should incentivize alignment through tax, regulatory, and market mechanisms**,** rewarding companies that embed security, resilience, and ethical standards consistent with alliance principles (Farrell and Newman, 2019). Third, sustained public-private partnerships can institutionalize collaboration in areas such as AI governance, supply-chain security,

cyber defense, and emerging technologies, providing both influence and mutual benefit (WEF, 2020).

Fourth, sustaining engagement from leading technology firms and AI “titans” requires cultivating a narrative of global stewardship that aligns private ambition with collective security goals. These actors are often driven by legacy, reputational influence, and the broader societal impact of their technologies, meaning that NATO and allied governments can shape incentives by providing visible platforms that recognize contributions to global stability, disaster response, and humanitarian innovation (Nye, 2011; Zuboff, 2019). This helps frame participation in defense and security ecosystems not merely as commercial opportunity, but as a form of responsibility in shaping a resilient international order.

At the same time, the expansion of public–private collaboration must be balanced by robust ethical and governance frameworks, as growing civil society concerns around transparency, algorithmic bias, escalation risks, and autonomous decision-making highlight the need for strong safeguards such as auditability, meaningful human oversight, and strict compliance with international humanitarian law (Duffy, 2026). In turn, this kind of structured diplomatic and strategic engagement can help cultivate a shared understanding that market access, technological leadership, and geopolitical stability are mutually reinforcing, thereby aligning private-sector incentives more closely with both national and civil society security objectives and NATO’s collective security goals.

Important Strategic Mandates Supporting Digital Resilience and Foster Technical Partnerships

NATO has established institutional and consultative mechanisms to bring technology firms into its strategic orbit. Agencies such as the NATO Communications and Information Agency (NCIA) and Allied Command Transformation (ACT) convene industry roundtables, solicit input on capability development, and integrate civilian innovations into operational planning (NCIA, 2024). Concrete partnerships have also been formed with private companies providing operational capabilities: Finnish satellite operator ICEYE supplies Earth observation data to NATO’s Situation Centre, while Palantir Technologies’ AI-driven analytics platform enhances decision-making processes (Reuters, 2025; Financial Times, 2025). These collaborations illustrate a model in which NATO leverages commercial technology without ceding control, embedding resilience and operational continuity into critical systems.

NATO has already created some important strategies to support digital resilience. One of the principal mechanisms for this engagement is the NATO Innovation Fund (NIF), launched in 2022 and backed by 24 of the Alliance’s 32 member states (Coulter, 2024). The fund, with a target of over €1 billion, provides

venture-style investment in deep-tech firms capable of delivering capabilities relevant to defense and resilience. Early beneficiaries include Fractile, a British chipmaker optimizing large language models, Germany's ARX Robotics, a developer of unmanned robotics, iCOMAT, which produces lightweight materials for military vehicles, and Space Forge, a Welsh company producing semiconductors in orbit. By investing directly in these startups and partnering with venture capital firms, NATO is embedding itself within the innovation ecosystem, shaping technological trajectories while preserving the autonomy of commercial actors.

Furthermore, NATO has promoted structural alignment between corporate and Alliance priorities through accelerators and innovation ecosystems such as the Defense Innovation Accelerator for the North Atlantic (DIANA), which provides start-ups and researchers access to NATO test centers and technical infrastructure (NATO, 2021a). This integration ensures that innovation is dual-use, scalable, and aligned with both defense and humanitarian objectives, fostering a symbiotic relationship in which corporate actors gain access to strategic markets and NATO gains early insight into technological trends (Shea, 2022). Through these initiatives, the Alliance is cultivating an environment in which leading technologists are partners in collective security rather than isolated actors whose influence could destabilize the system (NATO, 2022a). By acting as a coordinating platform, NATO reduces fragmentation, strengthens collective defense, and helps countries—especially those with more limited resources—build capacity to safely, securely, and effectively integrate AI into their defense establishments (NATO, 2021b).

The NATO Cyber and Digital Transformation Division (CDT) constitutes a cornerstone of the Alliance's efforts to consolidate its strategic advantage in the emergent digital battlespace. By integrating advanced cyber capabilities with doctrinal innovation, the division enhances NATO's resilience against multifaceted threats (NATO, 2022b). Its remit extends beyond conventional military networks to encompass critical allied infrastructure, including energy systems, global trade corridors, data flows, and digital supply chains, reflecting an understanding that modern strategic competition is as much about information dominance as kinetic superiority (NATO, 2022c).

A central function of the CDT is cyber deterrence to pre-empt, deter, and respond to cyber-enabled threats emanating from both state actors and violent non-state organizations (NATO, 2022b). This involves continuous monitoring of threat landscapes, deployment of advanced intrusion detection systems, and the coordination of proactive countermeasures (Rid and Buchanan, 2015). In the context of transnational initiatives such as the Belt and Road Initiative (BRI), such capabilities ensure that adversarial exploitation of digital infrastructure does not translate into

strategic leverage against NATO or compromise the operational integrity of member states (Kavanagh et al., 2020).

At the same time, the division actively promotes the integration of emerging digital technologies—including artificial intelligence, autonomous systems, quantum-secured communications, and cloud-based analytics—into NATO's operational fabric (NATO, 2021c). By doing so, it enhances predictive threat modelling, accelerates decision-making cycles, and fortifies cyber resilience (Allen and Chan, 2017).

The CDT also functions as a nexus for intelligence exchange and coordinated cyber defense among NATO members and affiliated private-sector partners. Through real-time threat intelligence dissemination, collaborative incident-response frameworks, and joint exercises, the division reinforces a collective cybersecurity posture (NATO, 2022d). This cooperative paradigm is particularly salient in the BRI context, where infrastructure projects span multiple jurisdictions, and adversarial actors—including terrorist organizations and state-linked cyber actors—may seek to exploit gaps in cross-border cyber governance (Rolland, 2019).

Looking toward 2040, the Cyber and Digital Transformation Division recognizes the importance of NATO remaining committed to an anticipatory and adaptive digital strategy. The division must continue to urge the Alliance to confront an evolving spectrum of threats ranging from sophisticated state-sponsored cyber campaigns to decentralized terrorist operations by continuously recalibrating doctrine, operational tools, and collaborative mechanisms (NATO, 2022a). By prioritizing secure and responsible technological integration, NATO also closes potential digital loopholes that terrorists and hostile actors could otherwise exploit (UNODC, 2021).

Fostering Technology Partnerships in the Future

In the future, NATO might consider fostering technology partnerships. These could include creating a mechanism for countries to request strategic technology partnerships with the United States. (NATO, 2021; Farrell and Newman, 2019). Washington should create a framework for foreign governments to request strategic technology partnerships with the United States. Washington could lay out clear, broadly consistent criteria as a condition for these partnerships, such as robust intellectual property and cybersecurity protections and divestment from China-linked digital infrastructure (Segal, 2018; OECD, 2021). In exchange, Washington would fast-track approvals and support from bodies like the new U.S. Partnership Agency and expand technology trade missions, research collaboration, and talent exchanges (U.S. Department of State, 2025; White House, 2025).

Also useful, would be to strengthen and focus American AI Exports Program on key emerging markets. A July 2025 executive order on Promoting the Export of the

American AI Technology Stack requires industry proposals for a full-stack AI technology export package (White House, 2025). Given limited capacity and resources, the administration should focus the newly created program on priority emerging markets. The Economic Diplomacy Action Group empowered under the July 2025 executive order should undertake a comprehensive review of all relevant federal tools and resources to identify opportunities to streamline application procedures, requirements, and review timelines (U.S. Department of Commerce, 2025).

Also impactful would be to leverage NATO's influence over multilateral development banks to raise standards for all ICT projects. NATO and its allies should leverage their financial contributions to multilateral development banks, such as the World Bank and Inter-American Development Bank, to raise procurement standards to further emphasize quality, trust, and security, drawing on insights from the USTDA's Global Procurement Initiative (World Bank, 2022; USTDA, 2021).

NATO should convene a summit to explore opportunities for member-state sovereign wealth funds and other investment funds to support digital ecosystems in priority emerging markets. Canada, Denmark, Italy, Norway, and Türkiye—and perhaps, soon, the United States—have sovereign wealth funds. Norway's fund is the largest in the world, with $1.8 trillion in assets. (Sovereign Wealth Fund Institute, 2025).

Concluding Remarks

The balance of power is being rewritten not only by divisions as regards globalism and nationalism but by innovation itself — a technological order that redefines human potential. Who can innovate the fastest will design and determine the future. Perhaps not only chief innovating countries will drive innovation but perhaps AI itself -- who will ultimately be in control? Nations, industries, and individuals alike are reshaping their strategies to adapt to this shifting landscape, where data, algorithms, and sustainability are the new currencies of influence and power.

NATO has a powerful hand to play as emerging markets make generational policy, partnership and investment decisions for advanced digital infrastructure and services that have the potential to impact global security for generations to come. It is therefore important that NATO ensures that American and European tech companies remain close to their orbit. It will also be important to ensure that a good portion of the global technological ecosystems will remain rooted in democratic values and shared values of openness, freedom and rule of law (Chilukuri, Scanlon 2025). Failure to support these strategic alliances, could lead to a global technological world order that is no longer vigilant in keeping terrorists or criminal actors from abusing technology for nefarious purposes.

Over the coming twenty years, the NATO alliance will confront a strategic environment transformed by five interlocking global trends: the rise of national populism, rapid technological disruption, innovations in next-generation warfare, renewed great-power competition, and the erosion of the rules-based international order. Together, these forces will strain NATO's existing doctrines, challenge its institutional cohesion, and complicate its ability to counter evolving terrorist threats. The Alliance—and the wider Westphalian system of global governance—cannot manage these pressures in isolation; instead, adaptation will require new partnerships, flexible institutional frameworks, and a willingness to integrate non-state actors and Tech Titans into collective security architectures. This transformation is not merely tactical but fundamental, demanding a rethinking of military doctrine, governance, and the rule of law itself (Krepinevich, 94). As precision technologies proliferate and intelligent systems increasingly shape the conduct of war, NATO's central challenge will be preserving meaningful human control over violence while upholding the humanitarian principles that have underpinned international order for over a century (Grotius, 62). Preparing the Alliance for this future therefore requires a clear-eyed understanding of how emerging technologies will redefine power, sovereignty, and responsibility in twenty-first-century conflict—and whether NATO can evolve quickly enough to remain both militarily effective and normatively legitimate.

References

Abraham, D, Houmb, S.V, and Erdodi, L. Cyberattacks on Energy Infrastructure – A Literature Overview and Perspectives on the Current Situation, Applied Sciences, 22 August, 2025.

Abusix.com. "AI-Powered Vishing: Social Engineering with Deepfakes." 2025.

Al Arabiya English (2024) 'Underwater internet cables in Red Sea likely damaged after Houthis-downed ship', *Al Arabiya English*, 6 March.

Ahlander, J., Lehto, E. & Sytas, A. (2024) 'Two undersea cables in Baltic Sea cut, Germany and Finland fear sabotage', *Reuters*, 18 November 2024.

Allison, G., "*Destined for War: Can America and China Escape Thucydides's Trap?"* Boston: Houghton Mifflin Harcourt, 2017.

Allen, G. and Chan, T. "*Artificial Intelligence and National Security*." Cambridge, MA: Belfer Center for Science and International Affairs, 2017.

Al Jazeera (2026) 'Are drones, AI making it harder to fight armed groups in the Sahel?', *Al Jazeera*, 11 February.

Antonakakis, M., April, T., Bailey, M., et al. 'Understanding the Mirai Botnet', *USENIX Security Symposium*, 2017, pp. 1093–1110.

Arquilla, J. and Ronfeldt, D., *The Advent of Netwar*. Santa Monica, CA: RAND Corporation, 1999.

Arquilla, J. and Ronfeldt, D., *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation, 2001.

Australian Strategic Policy Institute, *Authoritarian narratives in the digital age*. Canberra: ASPI, 2023.

Horowitz, M.C. (2026) *The AI word of 2026 should be 'adoption'*. Council on Foreign Relations (CFR) report/perspective collection, 2026.

Baldwin, D.A. "*Power and International Relations: A Conceptual Approach*." Princeton: Princeton University Press, 2016.

Ballard, M., Song, G. and Zhu, T.,c*Satellite cybersecurity across orbital altitudes*, 2025.

2024 Baltic Sea submarine cable disruptions," *Wikipedia, The Free Encyclopedia*, 23 August 2025.

Bego, Katja, Ukraine's Operation Spider's Web is a game-changer for modern drone warfare. NATO should pay attention, Chatham House, updated 17 July, 2025.

Bertram, L. and O'Hara, K. 'Terrorist propaganda in the age of next-generation communications', *Studies in Conflict & Terrorism*, 2020, 43(12), pp. 1093–1112

Biddle, S., *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton: Princeton University Press, 2006.

Biggio, B. and Roli, F. 'Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning', *Pattern Recognition*, 2018, 84, pp. 317–331.

Binnie, J., 'Houthi UAV and missile capabilities', 2021, *Jane's Defence Weekly*, 58(12), pp. 4–7.

Borrion, H., Shand, C. and Macintosh, A. 'Cyber-enabled terrorism and emerging technologies: The case of 5G', *Terrorism and Political Violence*, 2020, 32(6), pp. 1234–1252.

Brandt, J. (2026) *Who will 'win' the AI race?* Council on Foreign Relations (CFR) report/perspective collection, 2026.

Bronk, J., Reynolds, N. and Watling, J., "*The Military Lessons of the Ukraine War."* London: Royal United Services Institute (RUSI), 2023.

Brunsden, J. and Peel, M. 'Baltic Sea cable incidents raise fears of hybrid sabotage', *Financial Times*, 10 October 2023.

Byman, D., *A High Price: The Triumphs and Failures of Israeli Counterterrorism.* Oxford: Oxford University Press, 2013.

Chatham House, Space, the final frontier for cybersecurity?

Check Point Research, 'BadBox: Multifunctional IoT Botnets and the Evolving Threat Landscape', *Check Point Research Reports*, 2021.

Chen, M., Ma, Y., Li, Y., Wu, D. and Zhang, Y. 'IoT Security: Challenges and Solutions', *Future Generation Computer Systems*, 2018, 83, pp. 1–10.

Chen, T.M., Liu, R. and Zhang, L. 'Supply Chain Attacks and Persistent IoT Botnets: A Security Assessment', *Computers & Security*, 2022, 113, 102534.

Chesney, R. and Citron, D.K. 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', *California Law Review*, 2019, 107(6), pp. 1753–1819.

Cheung, T.M. *Civil–Military Fusion and China's Technological Rise*. Washington, DC: Center for Strategic and International Studies (CSIS) 2021.

Chivers, C.J. and Schmitt, E., 'Insurgents in Iraq Learn to Build Bombs From Shrapnel to Electronics', *The New York Times*, 21 March 2007.

CISA, *Apache Log4j vulnerability guidance.* Washington, DC: Cybersecurity and Infrastructure Security Agency, 2021

Clark, D.D., Lehr, W. and Bauer, S. 'Interconnection in the Internet: The role of emergency routing and redundancy', *Telecommunications Policy*, 2019, 43(4), pp. 101–113.

Cockayne, J. and Lupel, A., *Armed Groups and Communication Infrastructure in Conflict Zones*. New York: Routledge, 2018.

Conti, M., Dehghantanha, A., Franke, K. and Watson, S. 'Internet of Things Security and Forensics: Challenges and Opportunities', *Future Generation Computer Systems*, 2018, 78, pp. 544–546.

Conway, M. 'Determining the role of the internet in violent extremism and terrorism', *Studies in Conflict & Terrorism*, 2017, 40(1), pp. 77–98.

Clarke, R.A. and Knake, R.K., "*The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats."* New York: Penguin, 2019.

CSIS "*Emerging Trends in Jihadist Cyber Operations*." Washington, DC: Center for Strategic and International Studies, 2025.

CrowdStrike, *Sunburst: detecting and remediating the SolarWinds compromise*. Austin, TX: CrowdStrike, 2020.

“Could the Houthis sabotage international internet cables in the Red Sea?”, *Naval-Technology.com*, [online], published date not specified.

David versus Goliath: How Technology is Changing Warfare, Council on Foreign Relations (CFR), 2024.

Cuyckens, Hanne**,** Foreign Fighters and the tension between counterterrorism and international humanitarian law: A case for cumulative prosecution, when possible, IRRC, No. 916-917, February 2022.

Cybersecurity and Infrastructure Security Agency (CISA) (2025) *Official Website of the Cybersecurity and Infrastructure Security Agency*.

Cloudflare (2024) ‘Resilient Internet connectivity in Europe mitigates impact of Baltic cable cuts’, *Cloudflare Blog*, 20 November.

CrowdStrike. “AI Threats and the Rise of Dark Web LLMs.” 2025

DiResta, R. (2023) *The digital influence machine*. New York: Harper.

East Asia Forum, *The growing threat of cybercrime in the space domain*. East Asia Forum, 9 September, 2021, https://eastasiaforum.org/

ENISA (European Union Agency for Cybersecurity) *Internet of Things Security Threat Landscape*. Heraklion: ENISA, 2021

ENISA *Threat Landscape for Subsea Communications Infrastructure*. Heraklion: ENISA, 2022.

Esteva, Andre, et al. “A Guide to Depp Learning in Healthcare.” Nature Medicine, vol. 30, no. 2, 2024, pp 320-330.

Euronews & AP ‘What do we know about internet disruptions from cut subsea cables in the Red Sea’, *Euronews Next*, 8 September 2025.

European Union Agency for Cybersecurity (ENISA) *5G Threat Landscape and Security Recommendations*. Heraklion: ENISA, 2020.

Europol, “*Changes in Modus Operandi of Islamic State Terrorist Attacks.”* The Hague: Europol, 2016

Europol, *Internet Organized Crime Threat Assessment (IOCTA) 2021*. The Hague: Europol, 2021.

Farrell, H. and Newman, A.L. ‘Weaponized interdependence: How global economic networks shape state coercion’, *International Security*, 2019, 44(1), pp. 42–79.

Financial Times, "Ukraine's Asymmetric Strike Capability Demonstration," June 14, 2025, 4.

Finlayson, S.G., Bowers, J.D., Ito, J., Zittrain, J.L., Beam, A.L. and Kohane, I.S. 'Adversarial Attacks on Medical Machine Learning', *Science*, 2019, 363(6433), pp. 1287–1289.

Freedman, L. *Ukraine and the Art of Strategy*. Oxford: Oxford University Press, 2022.

Galeotti, M. "*Hybrid War or Gibridnaya Voina? Getting Russia's Non-linear Military Challenge Right".* Rome: NATO Defense College, 2016.

Galeotti, M. 'Russia's wars: Old doctrine, new realities', *Survival*, 2022, 64(2), pp. 7–28.

Galula, D., "*Counterinsurgency Warfare: Theory and Practice,"* Westport, CT: Praeger, 2006.

Gholz, E. 'Rare earth elements and national security', *International Security*, 2021, 45(3), pp. 7–43.

Gorwa, R., Binns, R. and Katzenbach, C. Algorithmic content moderation: Technical and political challenges in the automation of platform governance', *Big Data & Society*, 7(1), 2020, pp. 1–15.

Grotius, Hugo, *The Law of War and Peace*, trans. Francis Kelsey (Indianapolis: Bobbs-Merrill, 1962), foundational principles still relevant to modern warfare ethics.

Han, R. 'Manufacturing consent in the digital age: China's online influence operations', *Journal of Contemporary China*, 31(136), 2022, pp. 555–572.

Hoffman, F.G. "*Conflict in the 21st Century: The Rise of Hybrid Wars*." Arlington, VA: Potomac Institute for Policy Studies, 2007.

Hoffman, B., *Inside Terrorism.* 2nd edn. New York: Columbia University Press, 2006.

Hoffman, F.G. 'Learning in Modern Asymmetric Conflict', *Journal of Strategic Studies*, 2006, 29(1), pp. 55–92.

Hoffman, F.G. 'The Wagner Group and Russian Power Projection', *Small Wars Journal*, 2021, 17(4), pp. 1–15.

Howard, P.N., Ganesh, B., Liotsiou, D., Kelly, J. and François, C. "*The IRA, social media and political polarization*." Oxford: Oxford Internet Institute, 2018.

Humphries, M., "*Rare earth elements: the global supply chain"*. Washington, DC: Congressional Research Service, 2019.

IBM X-Force Research, IoT Threat Horizons: Machine-Learning–Driven Malware and Emerging Techniques. Armonk, NY: IBM Security 2023.

International Institute for Strategic Studies (IISS) "*The Strategic Impact of Unmanned Systems in the Russia–Ukraine War*." London: IISS 2024.

International Telecommunication Union (ITU) *Resilience of Submarine Cables in the Context of Climate Change and Security Risks*. 2021, Geneva: ITU.

ISS Africa (2025) ‘Sahel militants turn civilian drones into deadly weapons’, *ISS Today*, 8 July.

Janjeva, A., Gausen, A., Mercer, S. & Sippy, T. (2024) *Evaluating Malicious Generative AI Capabilities: Understanding inflection points in risk*. CETaS Briefing Papers, July.

‘Joint statement by the Foreign Ministers of Finland and Germany on the severed undersea cable in the Baltic Sea’ (2024) *Federal Foreign Office – Germany*, 18 November.

Jones, D. Cybersecurity Dive. “Massive Iran Linked Botnet Launches DDoS Attacks against telecom and gaming platforms.” 3 March 2025.

Jones, D. Cybersecurity Dive, “More than 86K IoT devices compromised by fast-growing Eleven11 botnet, 5 March 2025.

Kaldor, M. “*New and Old Wars: Organised Violence in a Global Era*.” 3rd edn. Cambridge: Polity Press, 2012.

Kania, E.B. ‘AI weaponization and the future of great power competition’, *Texas National Security Review*, 2020, 3(2), pp. 57–80.

Kavanagh, J., Marcellino, W., Blake, J.S. and Smith, S. *“Countering China’s Digital Silk Road.”* Santa Monica, CA: RAND Corporation, 2020.

Kietzmann, J., Lee, L., McCarthy, I.P. and Kietzmann, T.C. ‘Deepfakes: Trick or Treat?’, *Business Horizons*, 2020, 63(2), pp. 135–146.

Kilcullen, D., “*The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One.”* Oxford: Oxford University Press, 2009.

Knights, M., ‘The Houthi war machine’, 2020, *CTC Sentinel*, 13(8), pp. 1–14.

Kofman, M., Lee, R. and Connolly, R. (2023) *Russia’s war in Ukraine: military adaptation and innovation*. London: RUSI.

Koné, H. and Koné, F.R. (2025) ‘Sahel militants turn civilian drones into deadly weapons’, *ISS Africa*, 8 July.

Kshetri, N., ‘The Strategic Importance of Securing IoT Devices in Critical Infrastructure’, *Telecommunications Policy*, 2021, 45(9), 102176.

Kshetri, N. ‘5G Networks and Cybersecurity Challenges for Non-State Actors’, *Telecommunications Policy*, 2021, 45(9), 102176.

Krepinevich, A.F., "The Military-Technical Revolution," *The National Interest*, no. 37 (Fall 1994): 23-31.

Krepinevich, A.F. "*The Military-Technical Revolution: A Preliminary Assessment*." Washington, DC: Center for Strategic and Budgetary Assessments, 1994.

Kello, L., *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), 12.

Lewis, J.A., *China's Strategic Emerging Industries and Technological Development*. Washington, DC: Center for Strategic and Budgetary Assessments, 2018.

Li, X. and Zhang, Y. 'The strategic implications of 5G for national security', *Journal of Strategic Studies*, 2021, 44(6), pp. 857–879.

Lin, H. and Berg, H. 'Asymmetric Threats in IoT-Enabled Systems: Lessons from Mirai and BadBox', *Journal of Cybersecurity*, 2020, 6(1), pp. 1–15.

McGuire, C. (2026) *The year AI hype becomes a reality*. Council on Foreign Relations (CFR) report/perspective collection, 2026.

Monaghan, S., Darrah, M., Jakobsen, E. & Svendsen, O. (2024) 'Red Sea Cable Damage Reveals Soft Underbelly of Global Economy', *Center for Strategic & International Studies*, 7 March.

Mueller, R.S., *Report on the investigation into Russian interference in the 2016 presidential election*. Washington, DC: U.S. Department of Justice, 2019.

National Institute of Standards and Technology (NIST) *IoT Device Security Guidelines and Best Practices*. Gaithersburg, MD: NIST, 2021.

National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, DC: Government Printing Office, 2004

NATO "*Defence Innovation Accelerator for the North Atlantic" (DIANA): Factsheet.* Brussels: NATO. (2021a).

NATO "*NATO Artificial Intelligence Strategy"*. Brussels: NATO. (2021b).

NATO "*Emerging and Disruptive Technologies Roadmap*." Brussels: NATO. (2021c).

NATO Maritime Command, *Maritime Domain Awareness and the Protection of Critical Infrastructure*. Northwood: NATO MARCOM, 2022.

NATO "*Strategic Concept 2022"*. Madrid: NATO. (2022a).

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2021) *5G Security in Multi-Domain Operations*. Tallinn: CCDCOE.

NATO "*Cyber Defence Policy*." Brussels: NATO. (2022b).

NATO "*Resilience and Critical Infrastructure Protection*." Brussels: NATO. (2022c),

NATO “*NATO Cyber Defence Pledge*.” Brussels: NATO, (2022d).

NATO “*NATO 2022 Strategic Concept.2* Brussels: NATO, 2022.

NATO, *Resilience of Critical Undersea Infrastructure*. Brussels: NATO Headquarters, 2023

NATO - *NATO 2030: United for a New Era*. Brussels: NATO, 2021.

Nova, A. “Weaponized AI Malware and Threat Adaption.” 2025

Nye, J.S., *The Future of Power.* New York: PublicAffairs, 2011.

Nguyen, T.T., Nguyen, C.M., Nguyen, D.T., Nguyen, D.T. and Nahavandi, S. ‘Deep Learning for Deepfakes Creation and Detection: A Survey’, 2019, *arXiv preprint arXiv:1909.11573*.

Nguyen, V.X. (2026) *The growing AI trust gap is a national security issue*. Council on Foreign Relations (CFR) report/perspective collection, 2026.

O’Boyle, C. and Lanoszka, A. ‘Sanctions as Asymmetric Tools of Coercion: Lessons from Russia and Ukraine’, *Journal of Strategic Studies*, 2022, 45(6), pp. 912–936.

OECD *Principles for the Governance of Critical Digital Infrastructure*. Paris: OECD 2021.

Okpaleke, F.N., Nwosu, B.U., Okoli, C.R. and Olumba, E.E. (2023) ‘The case for drones in counter-insurgency operations in West African Sahel’, *African Security Review*, 32(4), pp. 351–367.

Özgen, C., & Kurt, S. (2025). PKK's drone attacks within the perspective of learning organisation and Türkiye's counter reaction. *Bulletin of "Carol I" National Defence University*, 14(2), pp. 93-113.

Patel, P. Impact of IoT Security on Different Domains 2025, eInfochips Blog, 5 August, 2025.

Petraeus, D. and Amos, *The U.S. Army and Counterinsurgency: Field Manual No. 3-24.* Washington, DC: Department of the Army, 2006.

Polyakova, A. and Meserole, C. ‘Exporting Digital Authoritarianism: The Russian and Chinese Tech Models’, *Brookings Institution Report*. Washington, DC: Brookings, 2019.

Polyakova, A. and Meserole, C., ‘The Information Front in the Ukraine Conflict’, *Brookings Institution Report*. Washington, DC: Brookings, 2022.

PwC, Satellite cybersecurity, PriceWaterhouseCooper, https://www.pwc.com/

Reuters (2025) ‘Surge in attacks signals jihadist comeback in Nigeria’s northeast’, *Reuters*, 29 April.

Rid, T., “*Active measures: the secret history of disinformation and political warfare.”* New York: Farrar, Straus and Giroux, 2020.

Rid, T. and Buchanan, B. (2015) ‘Attributing cyber attacks’, *Journal of Strategic Studies*, 38(1–2), pp. 4–37.

Rid, T., *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013

Rinaldi, S., McDaniel, P. and Van Meter, R. (2020) ‘5G Networks and Critical Infrastructure: Security Implications’, *IEEE Communications Magazine*, 58(4), pp. 24–30.

Risk Bulletins, *Risk Bulletins: Security and Technology Analysis Reports 2025*.

Rolland, N. *“China’s Eurasian Century? Political and Strategic Implications of the Belt and Road Initiative.”* Seattle: National Bureau of Asian Research, 2019.

Rose, K., Eldridge, S. and Chapin, L. *The Internet of Things: An Overview*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2015.

Roman, R., Zhou, J. and Lopez, J. ‘On the Features and Challenges of Security and Privacy in Distributed Internet of Things’, *Computer Networks*, 2013, 57(10), pp. 2266–2279.

RUSI, “*Deep Strike and Covert Operations in Ukraine*.” London: RUSI, 2024.

RUSI, “*The Russian–Ukrainian War and the Future of Covert and Hybrid Operations.”* London: Royal United Services Institute, 2023.

Salhani, J. ‘Why are people blaming Yemen’s Houthis for cutting the Red Sea cables?’, *Al Jazeera*, 6 March 2024.

Sallama, M.B. (2026) ‘Drone warfare by jihadist groups in West Africa: A growing threat’, *Modern Ghana*, 10 February.

Satellite Today “Intelsat shuts down transponder hijacked by terrorists”, 2007, https://www.satellitetoday.com/

Segal, A. *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Washington, DC: Carnegie Endowment for International Peace, 2018.

Segal, A. *Keep a close eye on China’s AI efforts*. Council on Foreign Relations (CFR), 2026.

Segal, A., *The Hacked World Order: How nations fight, trade, maneuver, and manipulate in the digital age.* New York: PublicAffairs, 2020.

Schmitt, M.N. ‘Autonomous weapon systems and international humanitarian law’, *Harvard National Security Journal*, 2019, 10, pp. 1–24.

“Shadow fleets” and subaquatic sabotage: are Europe’s undersea internet cables under attack?’ (2025) *The Guardian*, 5 March.

Shea, J. ‘NATO’s technological edge and innovation partnerships’, *NATO Review*, 2022, 70(2), pp. 1–10.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. ‘Security, Privacy and Trust in Internet of Things: The Road Ahead’, *Computer Networks*, 2015, 76, pp. 146–164.

Simonovich, Vitaly, CATO CTRL™ Threat Research: Analyzing LAMEHUG – First Known LLM-Powered Malware with Links to APT 28 (Fancy Bear). https://www.catonetworks.com/blog/cato-ctrl-threat-research-analyzing-lamehug/

Singer, P.W. and Friedman, A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014.

Smith, R. and Jones, T. ‘Sabotage and terrorism targeting telecom infrastructure’, *Global Security Review*, 2021, 8(3), pp. 45–59.

Sovereign Wealth Fund Institute (2025) *Sovereign Wealth Fund Rankings*.

Space and Defense Trends Analysis, Space terrorism future trends analysis, 2025.

Soneye, Oluwaseyi, Detecting and Responding to Funklocker Ransomware with Wazuh, Wazuh Blog, 22 November 2025.

SQMagazine.co.uk. “AI in Ransomware 2025: Autonomy and Threats.” 2025

Starosielski, N., *The Undersea Network*. Durham, NC: Duke University Press 2015.

Stockhammer, (2026) *Soufan Centre,*

Symantec Threat Intelligence, ‘The Evolution of IoT Malware: From Mirai to Modern Threats’, Mountain View, CA: Symantec, 2022.

Thévenin, P. ‘A legislative route to combat sabotage of undersea cables: A Q&A with Pierre Thévenin’, *Stockholm International Peace Research Institute Commentary / Topical Backgrounder*, 23 October 2025.

Tooze, A., *Shutdown: How Covid Shook the World’s Economy*. London: Allen Lane 2021.

Trend Micro,‘BadBox Malware Targets Android Devices via Supply-Chain Compromises’, *Trend Micro Security Intelligence*. 2022.

US Department of Commerce, *Export Control Policy on Advanced Semiconductor Technologies*. Washington, DC: Bureau of Industry and Security, 2023.

U.S. Department of Commerce, *Economic Diplomacy Action Group: Annual Report*. Washington, DC: U.S. Department of Commerce, 2025.

U.S. Department of State, *U.S. Technology Partnerships Program: Policy Brief*. Washington, DC: U.S. Department of State, 2025.

United States Trade and Development Agency (USTDA) *Global Procurement Initiative: Strengthening ICT Standards*. Washington, DC: USTDA, 2021.

UNODC, "*Cybercrime and Terrorism": The Use of Information and Communication Technologies by Extremist Organisations."* Vienna: United Nations Office on Drugs and Crime, 2024.

UNODC, "*The Use of the Internet for Terrorist Purposes*." Vienna: United Nations Office on Drugs and Crime, 2021.

United Nations General Assembly, *United Nations Convention on the Law of the Sea*, Articles 113–115, 1982.

'Undersea power cable linking Finland and Estonia hit by outage, prompting investigation' (2024) *Associated Press*, 25 December.

United Nations (2025) *United Nations Official Website*.

U.S. Senate, "*Intelligence Committee report on the SolarWinds cyber intrusion*." Washington, DC: U.S. Government Publishing Office, 2021.

Varonis Threat Labs. "WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks." Varonis Blog, 29 October, 2025.

Venable, D.,**'**Forget guerrillas and IEDs: The next asymmetric war will be engineered', *The Cipher Brief*, 'A Chinese-Flagged Ship Cut Baltic Sea Internet Cables' (2024) *Carnegie Endowment for International Peace*, 3 December, 2024.

Venable, D., (2024) *Synthetic Asymmetry: Engineering technological advantage in modern conflict*. London: Routledge, 2024.

Vaccari, C. and Chadwick, A. (2020) *Deepfakes and Disinformation: Exploring the Impact on Political Communication*, Oxford: Oxford Internet Institute.

Venable, H. 'Synthetic Asymmetry and the Future of Conflict', *Journal of Strategic Studies*, 2022, 45(5), pp. 721–742.

Watling, J. and Reynolds, N. "*Ukraine at war: from survival to victory?"* London: Royal United Services Institute, 2022.

West, D. M. (2021) *Digital Government: Technology and public sector performance*. Washington, DC: Brookings Institution Press.

Weimann, G., *Terrorism in Cyberspace: The Next Generation*. Washington, DC: Columbia University Press, 2015.

Westerlund, M. ‘The Emergence of Deepfake Technology: A Review’, *Technology Innovation Management Review*, 2019, 9(11), pp. 39–52.

White House, *Executive Order on Promoting the Export of the American AI Technology Stack*. Washington, DC: The White House, 2025.

Will Kirkman et al., “Current- and Future-State Legacy Semiconductor Manufacturing Capacity,” MITRE, May 24, 2024.

Woolf, Nicky, DDoS attack that disrupted the internet was the largest of its kind in history, experts say, The Guardian, 26 October 2015.

World Bank, Procurement Guidelines for ICT Projects in Emerging Markets. Washington, DC: World Bank. 2022.

World Economic Forum (WEF) (2020) *Public–Private Cooperation in Cybersecurity*. Geneva: WEF.

Xu, X., He, Q., & Zhang, X. ‘Edge Computing, Network Slicing and Security Challenges in 5G’, *IEEE Network*, 2021, 35(2), pp. 112–119.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014) ‘Internet of Things for Smart Cities’, *IEEE Internet of Things Journal*, 2014, 1(1), pp. 22–32.

Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York: Crown, 2014.

Zuboff, S. (2019) *The Age of Surveillance Capitalism*. New York: PublicAffairs.

CHAPTER 2

What's Next for Terrorist Strategies?

Prof. John Arquilla

Abstract

Our understanding of terrorists, and the future courses of action they may pursue, can be improved by recalling that, beyond its morally reprehensible characteristics, terrorism is at heart a form of warfare. By accepting this, we open up opportunities to think through terrorist strategies. Much like leaders of nations at war, terrorists think in terms of the scope and scale of operations. For example, Osama bin Laden thought about striking the "far enemy" half a world away in large-scale actions on 9/11, killing thousands and causing economic damage measured in the hundreds of billions of dollars. Today, however, most terrorist organizations appear focused on a strategy crafted by Abu Mus'ab al-Suri, a colleague of bin Laden's, who focused on smaller-scale attacks, though these can – al-Suri thought should – be conducted or supported over a wide geographic scope of action. For all the prevalence of the trend toward al-Suri's thinking about "scaling out" small terrorist acts around the world, it is possible that terrorists are now once again thinking about how to "scale up" the intensity of operations. The return of Afghanistan as a haven from which to engage in fresh thinking about future strategies, and the apocalyptic visions of some extremist groups, fed by their familiarity with advanced technologies (e.g. DNA synthesizers that can be used to craft deadly new pathogens), suggest the possibility that a sharp rise in the scale of terrorism may be in store. With scale measurable both in terms of heavy loss of life and massive economic disruption.

Introduction

One of the more vexing ironies of the early decades of the 21st Century is that the "global war on terror" proclaimed by President George W. Bush in the wake of the attacks on America in September 2001 has morphed into terror's war on the world. By all measures, there is far more terrorism – the vast majority of it comprised of violence aimed at civilian targets – being perpetrated today than there was prior to 9/11. The principal sources of the upsurge in terror are religiously motivated groups, like al Qaeda and its affiliates, and DAESH, that account for most of the injuries and fatalities. And their dark causes have thrived, despite the concerted efforts of the leading nations of the world to extirpate them. The statistics that best note the rise of this source of

terrorism can be found in Dominique Reynié's (2024) sweeping summary of all Islamist groups' actions over nearly the past half-century. As the report he oversaw notes, from 1979-2000, terrorism by violent extremist groups (some claiming Islamic justification) caused nearly 7,000 deaths. This figure rose more than five-fold, to 38,000 from 2001-2012, jumping to 200,000 fatalities from 2013-2024. Aside from the sheer, shocking rise in the lethality of terrorism since 2001, it is deeply troubling that so much of the carnage was wrought in those countries where the United States and its allies chose to intervene militarily: Afghanistan and Iraq. The former now once again serves as a haven for terrorists, the latter has become an unstable, hothouse-like environment breeding fresh perils. Tragic developments demanding serious, sustained attention.

Thus, despite the world's current focus on problems of great-power politics like the return of an aggressive Russia and the economic and military rise of China as threats to global stability, the continuing spread of terrorism, particularly of the Islamist variety – almost all sixty terrorist groups officially recognized by the UN are violent extremist organisations that misappropriate religious rhetoric that account for the majority of attacks, should not be neglected. Especially since diversion of attention away from terrorist networks allows them the breathing space to craft new organizational forms, concepts of operations, and strategies. This essay aims to refocus attention on terrorist organizations, with an emphasis on the range of strategic possibilities that lie before them.

Perhaps the most pertinent of the many definitions of terrorism that can help with the parsing of strategy is Richard English's (2009, pp. 23-4), which includes all the usual tropes regarding the use of "heterogeneous violence" employing "a variety of acts, of targets, and of actors . . . in the hope of maximizing political communication and achievement." But most important for strategic assessment purposes is his conclusion that terrorism "represents a subspecies of warfare." English argues that "there are numerous good reasons for defining terrorism within the context of war. Not only terrorists, but also their opponents have frequently seen themselves in these terms." This point about terrorism being perceived by both its adherents and its opponents as a form of war has also been affirmed by another of the leading scholars in the field, Mark Juergensmeyer (2008, pp. 75-6).

The notion of terrorism as a subspecies of warfare has replaced Walter Laqueur's early argument – when emblematic acts of terror consisted of plane hijackings, assassinations, and various forms of extortion – that terrorism "is not, as frequently believed, a subspecies of guerrilla (or 'revolutionary') warfare" (1977, p. 5). Later on, though, he accepted at least the idea that terrorism "shades on occasion into guerrilla warfare" (1996, p. 25), a realm that includes insurgents who, in their campaigns throughout history, have often employed acts of violence against noncombatants as well as attacks on adversary militaries. As Lewis Gann stated the matter presciently (1971, p. 86) regarding modern insurgents' practice of terrorism,

“the employment of terror against large numbers . . . seems to pay bigger dividends than assaults against a few highly placed men in the governmental hierarchy of the kind carried out by nineteenth century anarchists.” For violent extremist groups that misappropriate Islamic terminology, , this kind of warfare is falsely labeled as an aspect of so-called *jihad al-sayf,* “jihad of the sword” that, as Robinson (2021, p. 1) notes that these groups claim it is “religiously sanctioned armed violence carried out in defense of Islam, Muslim territory, or Muslim lives.” However, mainstream Islamic scholarship rejects this interpretation, as classical jihad rules prohibit killing non-combatants, suicide, and treachery (Qur’an 5:32, Al Azhar fatwa, 2015) And with regard to the irregular warfare tactics used by such groups –including suicide attacks (which Islamic law explicitly condemns as haram)- some scholars have drawn a historical parallel to Ibn Khaldun’s description of medieval Arab raiding tactics of “attack and withdrawal” (Khaldun, 1967, p.224). But this is a descriptive analogy, not a religious justification. Ibn Khaldun was observing military customs of his time, not sanctioning modern terrorism. Moreover, equating any historical Muslim warfare with contemporary terrorist violence ignores the fundamental differences in targets (combatants then vs. civilians today) and ethical frameworks**.**

It is important to note terrorists who claim religious justification are hardly the only terrorists who see what they do as acts of war or view themselves as warriors. From the outset of the era of modern terrorism, members of most groups have self-defined in terms of their being serving soldiers in war – albeit an irregular mode of war necessitated by the inability to strike enemies in a more conventional manner. The British journalist Gerald McKnight compiled one of the first cross-group studies (1974) of terrorist organizations worldwide, ranging at the time from the Irish Republican Army to Basque separatists, Greek Cypriots, Palestinians, Uruguayan Tupamaros, and the Japanese Red Army, to name some. He made a point during his interviews with these groups’ leaders and many fighters to explore the rationales for inflicting lethal violence on the innocent. While motives varied – some were fighting for the notion of a “homeland,” others had grander aims like the Japanese Red Army’s goal of global disruption, a foreshadowing of Aum Shinrikyo’s bizarre master plan a generation later – all saw themselves clearly as operating in the realm of warfare. All argued that the killing of innocents could lead to the end of greater injustices and save more lives in the long run. And almost all, across the world, asserted that their actions consisted of necessary responses to the outrages inflicted upon and killings of their own innocent people. As one IRA leader summed up a rationale repeated in various ways by many terrorists from other groups, their actions were “enforced, national resistance to naked aggression” (McKnight, 1974, p. 71).

With this notion of terrorism as a mode of warfare in mind, it seems clear that considering, hopefully anticipating, the range of possible strategies terrorist groups might choose is an important and worthwhile undertaking. Some excellent work has

already been done on this subject (Kydd and Walter, 2006), approaching it with a focus on terrorists' ultimate goals and some general means for pursuing them. Goals are categorized as: regime change or territorial acquisition; policy change or social control; or just maintenance of an acceptable status quo (pp. 54-55). As to achieving these aims, Kydd and Walter divide strategies (pp. 59-78) in two: those aimed at the enemy and those employed toward – or rather against – their own constituencies. The major strategy against enemies is attritional, in the hope of wearing down the will but also sometimes provoking the over-reaction of the counter-terrorists. As to strategies focused on supportive populations, these consist of a mix of either intimidating or inciting actions, often a mix of both.

Drawing together disparate views of earlier scholarship on terrorist strategy (e.g., Thornton, 1964; Fromkin, 1975; and Crenshaw, 1981), Kydd and Walter have provided a valuable framework for parsing the goals and operational approaches terrorist groups might pursue. But if we are to proceed from the perspective that terrorism is an aspect of warfare, then there is yet more to consider from a strategic angle. Especially the choices that have to be made by the terrorists about the scope and scale of the actions by which they intend to pursue their aims.

Thus, the focus of this essay is on how narrowly or widely a terrorist group plans to operate and the level of intensity – what mixture of large- and small-scale acts of violence – its members employ. To put these aspects of terrorist strategy simply, these are questions of *scope* and *scale.* Perhaps the simplest examples of these elements of terrorist strategy can be found in two of Jules Verne's memorable antagonists: the vengeance-driven Captain Nemo from *Twenty Thousand Leagues Under the Sea* (1870); and the utterly mad scientist Dr. Schultze from *The Begum's Millions* (1879). Nemo's true identity, that of an Indian prince who lost all during the 1857 rebellion against British rule, was revealed in Verne's *Mysterious Island* (1875). The terrorist campaign he waged against international maritime commerce from his submarine *Nautilus* endowed him with a global scope of operations. But his attacks were few and small in scale, damaging individual ships. He sank only the warship that finally caught up with him. On the other hand, Dr. Schultze, who hated the liberal ways of a neighboring city – located just on the other side of a mountain – developed a chemical weapon with which he hoped to kill its 250,000 citizens. His intentions were limited in scope but he aimed for effects on a massive scale. Thankfully, he failed. Verne was thus the first to speculate about terrorist use of a weapon of mass destruction. Interesting, as the term "terrorist" was first used at this time to describe such events as the assassinations of Czar Alexander II and President James Garfield, both in 1881, the former by a suicide bomber.

These illustrative fictional examples aside, Figure 1 provides a general sense of how "strategic space," depicted in terms of scope and scale, has been populated by actual terrorists from the recent past to the present. Al Qaeda for example, had

from early on a penchant for spectacular events that caused significant casualties and gained wide and sustained public attention, like the 1998 embassy bombings in Tanzania and Kenya that killed over 200 and wounded nearly 5,000. The group's attack on the *USS Cole* in 2000, was made on a military target, doing great damage to the ship but causing a far smaller number of casualties – just over 50 between those killed and wounded. But in 2001 al Qaeda greatly extended both the scope and scale of its operations, seizing control of four commercial airliners to strike at targets in New York and Washington, killing 3,000 and injuring – gravely and, due to toxic particulates, over time – several tens of thousands. Beyond direct damage, the economic impact of the attacks, conducted by 19 operatives, were staggering, with some estimates putting immediate costs in the $100 billion range ($40 billion in the form of insurance claims, the largest ever), and other effects – market losses, declining tourism income, lost jobs (over 400,000 in New York City alone) – that ran, by some estimates, as high as $2 trillion. Stiglitz and Bilmes (2008) added the costs the Afghan and Iraq wars incurred from 2001-2007, which they argued were direct reactions to the attacks on America, and came up with an additional impact of $3 trillion (see also: Makinen, 2002; Roberts, 2009; and Khimm, 2011).

But the swift American response to the 9/11 attacks, the invasion of Afghanistan a month later that toppled the Taliban regime and put al Qaeda on the run, forced Osama bin Laden and his senior advisers to shift away from actions of the widest scope and of the greatest possible scale of intensity. To be sure, there were still some smaller scale strikes against perceived "far enemies" conducted by local religiously motivated cells but guided by al Qaeda's core operatives. Perhaps the most notable of these actions was the set of suicide bombings in London in July 2005 that killed fifty-six and wounded 700. While the bombers were local Muslims who had been radicalized, it was discovered that training and guidance were provided by the al Qaeda core, an early foreshadowing of the kind of "franchising" that was soon to emerge. Indeed, in the case of Britain it grew clear by the end of the 2000s that "each of the major terrorist plots affecting the United Kingdom since the 9/11 attacks in the United States have had ties back to al Qaeda's central organization" (Brandon, 2009). And in the years since, as Figure 1 depicts, the franchises that have risen, in North, East, and sub-Saharan Africa – as well as in other locales – suggest that the current *modus operandi* of al Qaeda is to maintain and extend a very broad scope of relatively small-scale actions by nodes in its network that feature some guided by core operatives from the center and others with much looser affiliations.

This concept of operations closely mirrors the scope and scale called for by the leading al Qaeda strategic intellectual, Abu Mus'ab al-Suri (born Mustafa bin Abd Al-Qadir Setmariam Nasar). His *Global Islamic Resistance Call* focused on the building of widely dispersed cells in many countries able to take occasional small-scale action and was heavily influenced by Robert Taber's classic *The War of the Flea* (1965).

Brynjar Lia, whose biography of al-Suri includes fully translated chapters from the *Call* focusing on matters of scope and scale (2008, pp. 347-484), noted Taber's ideas from *The War of the Flea* were so salient that, during the last years of the 1990s when al-Suri taught at al Qaeda training camps in Afghanistan, "he gave many lectures based solely on this book" (p. 226). But for bin Laden, at the time, al-Suri's vision was insufficient; only attacks directly on the nation that bin Laden considered the greatest enemy of Islam would make for a truly effective strategy. And so he over-ruled al-Suri and proceeded on the path to 9/11, despite the fact that another principal voice in al Qaeda, that of Dr. Ayman al Zawahiri, was raised against waging a war over such an extended scope of operations and at such scale. Zawahiri argued that there were much more reachable "near enemies" supported by the United States, like Egypt, against whom tangible results were likely to be achieved. Still, al-Suri's and Zawahiri's preferred strategic approach had to wait until the wake of the American-led counterblows in Afghanistan and Iraq before their wide-scope, smaller-scale concept was embraced.

Another type of terrorist strategic path can be glimpsed in the evolution of DAESH over the past decade. This organization began with a relatively narrow scope of offensive operations in 2014, limited to parts of Syria and Iraq, but featuring a substantially higher scale that featured a significant mix of conventional military, irregular insurgent, and terrorist actions. Indeed, at one point early on, DAESH was threatening to advance on Baghdad. Its initial successes resulted from skillfully blending those three main types of violent action. This approach proceeded – perhaps unwittingly – along the lines of a model developed half a century earlier by Thornton. He argued that, in theory, it was better to operate like this, on "a continuum, with significant elements of terror and guerrilla warfare continuing through to the end" (1964, pp. 91-2) than to follow Brian Crozier's more sequential (and Mao-conforming) theory of rebellion that saw terrorism largely supplanted by insurgency, both forms then overtaken by conventional warfighting (1960, p. 163).

But the DEASH strategy of operating on a relatively narrow scope but a high scale of operations soon fell afoul of counterattacks led by Iranian- and American-supported military formations, the latter consisting primarily of terrorist groups that benefited greatly from the presence of U.S. military advisors. By 2017 DAESH forces found themselves outmatched and in full retreat, limited to small-scale guerrilla and terrorist actions in Iraq and Syria, no longer capable of holding territory. It was at this point that a profound shift occurred, with the organization refocusing itself as a primarily wide-scope operator and conductor of relatively small-scale acts of terrorism – the targets of which were to include Muslims who didn't adhere to the DAESH worldview. Colin Clarke's summary of the strategic shift DAESH was making at this time was apt: "What the world is witnessing is the transition . . . from an insurgent organization with a fixed headquarters to a clandestine terrorist network dispersed

throughout the region and the globe" (2017). As Figure 1 points out, this shift in scope by DAESH makes it, at the margin, even a bit more expansive than the current version of al Qaeda. Whether either of these organizations will ever return to planning and conducting larger-scale operations is a matter discussed in the final section of this chapter.

But first it is important to consider a few other salient terrorist groups – beyond al Qaeda, DAESH, and their affiliates – that have experimented with the scale or scope of their operations, or both. For example, the Houthis of Yemen for many years mostly confined the scope of their actions to the internal conflict in which they were embroiled, with occasional long-range missile or drone strikes against the Saudis who were supporting their adversaries. But in the wake of Hamas's military wing's large-scale attack on Israel in October 2023, the Houthis chose to expand the scope of their operations with drone and missile attacks on Israel and by striking at ships transiting the Red Sea – the latter actions compelling costly re-routing of vessels that increased the scale of effects.

Israeli and American retaliatory air strikes impelled the Houthis to tamp down their own attacks – much as IDF bombing of Hezbollah sites in Lebanon and Syria forced that terrorist group to curtail its own expanded scope and scale of operations. Needless to say, Hamas's military wing's jumped-up scale of operations against Israel brought down massive retaliation as well. Indeed, in each of these cases – Houthis, Hezbollah, and the military wing of Hamas the expanding the scope and/or scale of operations resulted in swift and severe retaliation. These results should be viewed in contrast to the mostly unimpeded success of al Qaeda and its affiliates, especially in sub-Saharan Africa, where expanded scope but relatively small-scale operations have ensued without provoking serious or sustained counter-interventions. In Afghanistan, the Taliban followed a successful strategy of small-scale actions, increasing their scope marginally, year on year, eventually winning back total control of the country.

The lesson here may be that small-scale operations of increasing scope may be the optimal approach for terrorists in the future. But will the experiences of the recent past that point to the greater efficacy of small-scale operations – of whatever scope – remain benchmarks for the future? The next section considers the notion that large-scale actions may, due to technological advances, come back into play in more effective ways. The chances that some antagonists in the ongoing new round of great-power rivalry may rekindle ties to terrorism, along the lines first described by Claire Sterling during the Cold War (1981), will also be considered.

Toward the Future of Terrorism

When one considers the scale aspect of the terrorist strategic space, the uppermost limit would be the realm of weapons of mass destruction – nuclear,

biological, and chemical. Thomas Schelling was among the first to think usefully about terrorism with nuclear weapons, starting with an observation about the attacks on Hiroshima and Nagasaki: “on the only occasion of the hostile use of nuclear weapons, they were used in a fashion that has to be considered terrorist” (1982, p. 67). He viewed the indiscriminate destruction that such weapons wrought as inherently terroristic, and so speculated about how the nonstate terrorist might ponder replicating what a nation (i.e., the United States) had chosen to do with this capability. Schelling thought such armament could prove attractive, asserting “that terrorist nuclear threats have a comparative advantage,” in part because a nonstate actor of this ilk “considers itself immune to reprisal because it has no homeland” against which to retaliate (p. 73). However, he thought the danger of terrorist acquisition of nuclear weapons was controllable, given that the cost and complexity of building an atomic bomb posed a huge “barrier to entry.” Which meant the principal concern would be to prevent down-streaming of such capability to terrorists from willing, conniving, or insufficiently secure nations. Thus, Schelling concluded “the best way to keep [nuclear] weapons and weapons material out of the hands of nongovernmental entities is to keep them out of the hands of national governments” (p. 76).

Schelling’s implicit endorsement of arms control treaties and weapons conventions went hand in hand with the daunting technological challenge that any terrorist group would face – and would still do so today – if it tried to make a nuclear weapon of its own. Additionally, as Jessica Stern has noted, there is a subset of motivations and capabilities that a terrorist group needs in order even to pursue a nuclear capability: a desire “to use the weapons despite formidable political costs ability to acquire or produce them, and . . . ability to deliver or disseminate them covertly . . . [T]he area created by the intersection of these sets is small” (Stern, 2000, p. 203). But Stern also observed that the number of terrorist groups that might meet her criteria could grow, especially in the areas of chemical and biological weapons where the barriers to entry were lesser. In these realms, the rise of increasingly powerful artificial intelligence (AI) could prove decisive in making the acquisition of these types of weapons of mass destruction easier. With regard to biological weapons, the emergence of AI-powered DNA synthesizers is especially troubling, given their low cost (a few tens of thousands of dollars) and ability to create, as Microsoft CEO Mustafa Suleyman has described the situation, “engineered pandemics” employing “novel pathogens far more transmissible and lethal than anything found in nature. These synthetic pathogens could evade known countermeasures, spread asymptomatically, or have built-in resistance to treatments” (Suleyman and Bhaskar, 2025, pp. 10, 12-13).

Suleyman also notes that advanced AI can have a similar effect on cyber weapons – viruses, worms, etc. – increasing their capabilities for inflicting “mass disruptive” effects on civil infrastructures. This would be a form of cyberterror that

imposes large-scale costs without causing great loss of life. But such levels of cyber sophistication could also circle back to Schelling's initial concern about nuclear terrorism for, as Andrew Futter has recently noted in his comprehensive study of this problem, "the risk that hackers might somehow breach or interfere with nuclear weapons and related systems has grown considerably" (Futter, 2018, pp. 9-10). Given that Russia has long employed a significantly automated "dead hand" nuclear launch authorization system (also known as "Perimeter") that can be activated if communications with the General Staff were severed, the cyber risk in this case is substantial. Perimeter, as one of its developers, Soviet-era military officer Valery Yarynich, put the matter, then goes into action "bypassing layers and layers of normal command authority" (Cited in Thompson, 2009). Which makes Russian nuclear command, control, and communications systems attractive targets for a terrorist organization with a desire to spark an apocalyptic nuclear exchange among the leading powers. And yet, while terrorist groups have long been using the internet and worldwide web for communications, coordination, recruitment and other functions, none have yet demonstrated master-level hacking capabilities.

That said, the Japanese terrorist group Aum Shinrikyo did indeed have apocalyptic goals and focused on developing chemical weapons that it tested in its sarin attacks on three Tokyo subway lines in 1995. Though soon after disbanded, Aum's successor, Hikari no Wa (a/k/a Aleph) is thought to retain some of its predecessor's ideas about the need for global disruption. And since Aleph is now focused on advances in information technology, Japan's authorities have continued surveillance on the group, based on its High Court's conclusion that "No major change is evident between Aum and Hikari no Wa" (Nippon News, 2019).

What of the possibility that some aggressive power might decide to send WMD "downstream" to a terrorist organization? While Claire Sterling's research during the Cold War showed a connection – though a debated and disputed one – between the USSR and some terrorist actions, these were mostly small-scale events like targeted assassinations (Sterling, 1981). She found that the Russians had no interest in passing the most mass-destructive weapons to terrorists. In my view, this will likely remain the case for Russia, China, Iran or other powers due to the risks of escalation and retaliation that would attend their sponsorship of a terrorist group enabled with WMD. Indeed, any major power courting terrorists would of necessity also have to worry that the group might turn on and threaten, blackmail, or even attack its nation-state supplier. Further, any state that was identified as having given a biological, chemical, or nuclear weapon to a terrorist group would immediately be viewed as a pariah and would be subject to military retaliation for any action with such weapons taken by the terrorists. Even in the case of Iran's close relationship with Hezbollah, for example, expert opinion at the RAND Corporation has concluded (e.g., see Nader, 2013) that leaders in Tehran would not incur the "massive risk" of "devastating

retaliation" (p. 29) if Iran ever acquired weapons of mass destruction of any kind and shared them with Hezbollah.

Despite the various strategic, political, and technological impediments to terrorists acquiring weapons of mass destruction – especially the unlikelihood of *any* nation-state passing such capabilities downstream to them – there is still the chance that some groups might pursue a path of developing arsenals with such capabilities on their own. While nuclear weapons will remain difficult to craft absent nation-state support, with the sole exception of smaller "dirty bombs" able at least to create radiological incidents, the chemical and biological realms will offer opportunities in the coming years. And not only those afforded by use of AI-driven DNA synthesizers, as noted above. For there is at least one organization, al Qaeda, that has re-established a secure haven in Afghanistan from which to plot and plan the development of future capabilities that marry large scale to the wide scope that the network already enjoys via its many affiliated groups. Al Qaeda has had a history of trying to develop radiological, chemical, and biological weapons, but these efforts proved fraught and generally unfruitful during its first period of haven in Afghanistan that ended with the American invasion in the fall of 2001 (Giorgidze and Wither, 2019). Long before, though, Cindy Combs pointed out that chemical and/or biological weapons may prove accessible, a threat to be taken seriously because "the reason that few groups have yet used such weapons rests upon the difficulty in disseminating the toxic substances in sufficient quantities. That is, surely, a frail defense" (Combs 1997, p. 133).

Indeed, al Qaeda's second period of haven in Afghanistan may yet prove beneficial to its research aimed at overcoming technical difficulties entailed in the development of toxins and pathogens. For it seems highly unlikely that the US, NATO, or any other combination of states will form up once again for an invasion and occupation of that sad land. And if al Qaeda succeeds at such an enterprise, it will truly have an ability to strike with large-scale effects, a complement to its distributed network of affiliates that operate on a narrow scope and small scale.

But beyond the difficult path to WMD acquisition or development, there may be other options for terrorist groups that desire to broaden their reach and intensify the scale of their operations. One very simple approach would be to insert terrorists into refugee/immigrant flow patterns, say for example in the southwestern United States or Europe, and then have them fan out and start wildfires during dry periods. Both these areas have suffered terribly from fires in recent years, and climate change will only exacerbate this problem. And all the terrorists need are books of matches and the ability to move around. Thus could al Qaeda, DAESH, or any other group increase both the scope and scale of operations – though scale in this instance would refer more to the massive economic effects of such actions, which would likely result in only incidental losses of life. In this case we have a dangerous riff on the traditional

defensive notion of “scorched earth” as a way to slow down an invader. Now the terrorist invader would do the scorching.

And if terrorists in the future do begin to shift toward thinking of scale effects more in economic terms rather than in numbers of people killed or injured there is the possibility of serious efforts being made to enhance cyberwarfare capabilities. For most terrorist groups cyberattack capabilities of this sort will remain elusive, as internal selection and development of already trusted operatives will take long years to come to fruition – with the attendant risks of discovery and monitoring of the chosen candidates’ connections. As to hiring cyber mercenaries, some groups also have to ensure religious devotion of the hackers they seek to hire. And nation-states must be very careful about using cyber mercenaries, as links back to a hacker’s state sponsor, tracked after a disruptive attack, could lead to escalation to open warfare. So, it might be that the most likely actors to seek the services of cyber mercenaries will be criminal cartels. The United States has recently (Fall 2025) designated them “foreign terrorist organizations” and has been taking military action against them – e.g., air strikes on seaborne drug shipments. Surely, leaders of drug cartels will have a natural impulse to craft retaliatory strategies; and they have ample resources with which to hire hackers. They can also keep them under close control, as hacking can be done at a distance from the infrastructure and other targets. And, as a US Secret Service agent put the matter, “Many of the [non-state] actors that we look at on a daily basis have capabilities that actually exceed the capabilities of most nation-states” (Maurer, 2018, p. xi).

Fig. 2

Possible Future Terrorist Strategies

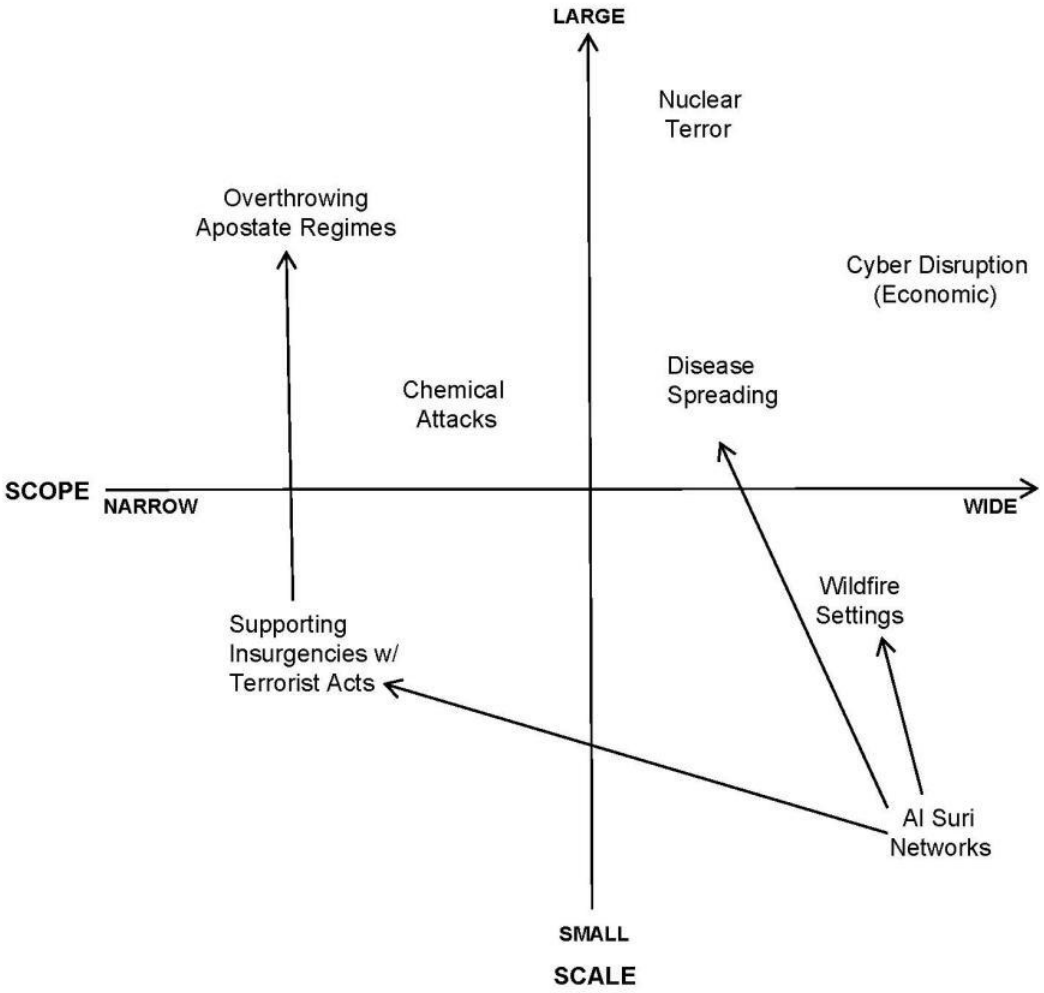


Figure 2 summarizes the potential future paths terrorist strategies might take, in terms of their scope and scale of operations. In many ways, this approach to analyzing what may be coming next identifies a possible terrorist third wave in the modern era. The first ranged roughly through the last decades of the Cold War (1970-1990), featuring terrorism that was for the most part narrow in scope and small in scale. The Lockerbie downing of a Pan Am flight in 1988 was a key exception hinting at the increasing scope and scale of terrorism that would soon emerge in a second wave, from 1991-2021, cresting with the 9/11 attacks in on the US in 2001and culminating twenty years later in restoration of Taliban rule and the al Qaeda haven in Afghanistan. This second wave of terrorism featured action of both broader scope and greater scale, with al Qaeda and DAESH – and affiliates – playing the most prominent roles. Strong military action taken by the US and its allies curtailed larger-scale depredations of these groups but did little to prevent the broadening scope of smaller-scale terrorist actions, conducted largely through their affiliated organizations and occasional “lone wolves.” And in the wake of the October 7, 2023 large-scale attack on Israel by Hamas’s military wing, the IDF’s retaliatory strikes, which extended also to attacks on Hezbollah, and the Houthis, forced these groups, for the most part, to “go to ground” and also to fall back on mounting smaller-scale insurgent and terrorist operations.

Indeed, it seems that the more likely future course of terrorism will reflect smaller-scale incidents – at least in terms of lives lost, but which may inflict significant economic damage – delivered across a wide scope of operations. From the afore mentioned fictional examples drawn from Jules Verne, this more disruptive approach would be less like the mass destruction that his "Dr. Schultze" sought and more like Captain Nemo's intention to undermine maritime trade, the source of the commercial wealth of the great empires of his time. Ray Bradbury called Nemo's approach – broad in scope, selective and small in scale – a "more constructive terror." Yet he admits Nemo, "like many reformers nevertheless winds up killing men to make them behave" (Bradbury, 1962, pp. 7,9). Even so, Nemo's disruptive actions inflicted little destruction, his only lethal "terror attack" coming against an armed naval vessel intent on *his* destruction.

Does Nemo's example suggest a possibility that a coming wave of terrorism might shift toward disruption rather than destruction? Given the risk that the near future might feature terrorists developing or otherwise acquiring WMD, we can only hope a Nemo-like choice for a "more constructive terror" is made. This will hardly mean terrorism without serious effect, as Nemo upended world commerce for a while, inflicting great financial losses. Cyberterror could do the same today. The hacking of the automaker Jaguar Land Rover's (JLR) supply-chain in August 2025 provides an example of how easily a major firm in an important industry can be disrupted. Due to dependence on a network of suppliers, once a link in JLR's chain was severed by cyberattack, the company had to shut down *all* operations for a month. Financial impact on the company quickly exceeded a quarter of a billion dollars. In addition, its 33,000 employees were idled, and serious effects were felt among the 100,000 workers in JLR's UK-based supply chain (Burgess, 2025).

While a coalition of cyber-criminal organizations claimed credit for this act, it should be considered as observationally equivalent to deliberate cyberterrorism – were actual terrorists to decide to begin focusing on "cybotage" with the aim of inflicting, then claiming credit for, such economic disruption. It doesn't take very much imagination to see that, if this sort of action could be undertaken repeatedly, a terrorist group could bring much attention to its cause. Since nobody would be killed, that cause might receive serious, perhaps at times even favorable, attention.

Roving teams of terrorist fire starters might not kill many people, but the destruction to trees, killing of wildlife, and the economic impact on cities located close to wildernesses would be massive – e.g., the 2025 Los Angeles wildfires have been estimated to have done damage in an amount higher than a quarter of a *trillion* dollars (Li and Yu, 2025). The increased heating and drying going on in some of the world's most productive economic zones, like Western Europe and North America, may make them increasingly attractive targets for this mode of disruptive terrorist attack. And while, as with cyber, losses of life when incurred from this type of action will be low,

the psychological impact of raging fires will be high, especially when people lose their homes and livelihoods when the fires reach more populated areas.

And there are yet other ways to mount broad scope, large-scale actions of a disruptive sort. Spreading infectious disease in humans and livestock, for example, could inflict enormous economic damage and serious losses of life among animals and people – depending on which would be targeted by any particular pathogen. On this point I won't mention any further details or other possibilities, as this essay is not intended as a "how to" but rather as a call to beware of what might be coming from future modes of terror. The point being that mass-disruptive modes of terrorism of the sort described herein can be undertaken by individuals, small teams, or cells in a way that allows for large-scale (but again, not particularly lethal, scale in this instance measured in terms of economic impact) actions of broad geographic scope.

In short, this possible future shift in the next wave of terrorism could be undertaken by small, scaled-down organizations that are nevertheless able to "scale out" across a world rich in soft targets and still all too easy to move throughout. In the case of cyberterror, particularly as practiced by criminal organizations that are newly labeled as terrorists, "movement" is a relative term, as such virtual attacks can be mounted from anywhere in the world. And even if forensics can identify the particular nonstate actor behind such depredations, deterrence will not work, given the amorphous nature of the perpetrator. Whereas, nation-states will likely prove loath to engage in or sponsor acts of cyberterror, given the risk discovery of culpability would surely result in a serious, if not massive, retaliatory response. Thus, the only way to cope with this threat is to focus on greatly improving the approach to cybersecurity, particularly by means of the ubiquitous use of strong encryption and by regularly moving key data around – e.g., in the Cloud or among the "edge devices" that constitute "the Fog." For data at rest are data at risk. As to spreading disease, this will likely require individuals to carry pathogens into the "target zones," which affords an opportunity to rethink the ease of movement many nations allow (especially in the European Union). The possibility that bioterrorists might follow paths taken by ordinary illegal immigrants implies a need to think, increasingly, of border security as central to *international* security.

In short, the time is now to engage in forethought about future terrorism.

References

Asprey, Robert (1994). *War in the Shadows.* New York: William Morrow & Co. Revised and updated from the first edition (1975).

Bradbury, Ray (1962). "The Ardent Blasphemers," Introduction to Jules Verne's *Twenty Thousand Leagues Under the Sea.* New York: Bantam Books.

Brandon, James (2009). "Al Qaeda's Involvement in Britain's 'Homegrown' Terrorist Plots." *CTC Sentinel,* Vol. 2, No. 3 (March). At https://ctc.westpoint.edu.

Burgess, Matt (2025). "A Cyberattack on Jaguar Land Rover Is Causing a Supply Chain Disaster." *WIRED,* September 22. Accessed at: www.wired.com.

Combs, C. (1997). *Terrorism in the Twenty-First Century.* Upper Saddle River, NJ: Prentice-Hall, Inc.

Clarke, Colin P. (2017). "How ISIS Is Transforming." *Foreign Affairs,* September 25, 2017. Accessed at: https://www.foreignaffairs.com.

Crenshaw, Martha (1981). "The Causes of Terrorism," *Comparative Politics,* Vol. 13, No. 4 (July), pp. 379-99.

Crozier, Brian (1960). *The Rebels: A Study of Post-War Insurrections.* London: Chatto and Windus.

English, Richard (2009). *Terrorism: How to Respond.* Oxford: Oxford University Press.

Fromkin, David (1975). "The Strategy of Terrorism," *Foreign Affairs,* Vol. 53, No.4 (July), pp. 683-698.

Futter, Andrew (2018). *Hacking the Bomb: Cyber Threats and Nuclear Weapons.* Washington, DC: Georgetown University Press.

Gann, Lewis (1970). *Guerrillas in History.* Stanford: Hoover Institution Press.

Giorgidze, Lasha, and James K. Wither (2019). *Horror or Hype: The Challenge of Chemical, Biological, Radiological, and Nuclear Terrorism.* Garmisch-Partenkirchen, Germany: George C. Marshall European Center for Security Studies, Publication No. 031. Accessed at: https://www.marshallcenter.org.

Juergensmeyer, Mark (2001). *Terror in the Mind of God: The Global Rise of Religious Violence.* Berkeley: University of California Press.

Khaldun, Muhammad ibn (1967[c.1377]). *The Muqaddimah: An Introduction to History.* Princeton: Princeton University Press. Translated by Franz Rosenthal.

Khimm, Suzy (2011). "Osama bin Laden Didn't Win, But He Was 'Enormously Successful'," *The Washington Post* (May 3).

Kydd, Andrew H., and Barbara F. Walter (2006). "The Strategies of Terrorism," *International Security,* Vol. 31, No. 1 (Summer), pp. 49-80.

Laqueur, Walter (1977). *Terrorism.* Boston: Little, Brown and Company.

_____(1996). "Postmodern Terrorism," *Foreign Affairs,* Vol. 75, No. 5 (September-October), pp. 24-36.

Li, Zhiyun, and William Yu (2025). *Economic Impact of the Los Angeles Wildfires.* Los Angeles: University of California Report, Anderson School of Management. Accessed at: www.anderson.ucla.edu.

Lia, Brynjar (2008). *Architect of Global Jihad: The Life of Al-Qaida Strategist Abu Mus'ab al-Suri.* New York: Columbia University Press.

Makinen, Gail (2002). *The Economic Effects of 9/11: A Retrospective Assessment.* Washington, DC: Congressional Research Service.

Maurer, Tim (2018). *Cyber Mercenaries: The State, Hackers, and Power.* Cambridge: Cambridge University Press.

McKnight, Gerald (1974). *The Terrorist Mind.* New York: The Bobbs-Merrill Company, Inc.

Mendelsohn, Barak (2016). *The Al-Qaeda Franchise: The Expansion of Al-Qaeda and Its Consequences.* Oxford: Oxford University Press.

Nader, Alireza (2013). *Iran After the Bomb: How Would a Nuclear-Armed Tehran Behave?* Santa Monica: RAND.

Nippon News (2019). "Tokyo Court Backs Extended Surveillance of Aum-Linked Group," (February 28). Accessed at: https://www.nippon.com.

Reynié, Dominique (2024). *Islamist Terrorist Attacks in the World, 1979-2024.* Paris: Fondation pour l'innovation politique. All data can also be accessed at: https://www.fondapol.org.

Roberts, Bryan W. (2009). *The Macroeconomic Impacts of the 9/11 Attack: Evidence from Real-Time Forecasting.* Washington: Department of Homeland Security (August).

Robinson, Glenn E. (2021). *Global Jihad: A Brief History.* Stanford: Stanford University Press.

Schelling, Thomas C. (1982). "Thinking About Nuclear Terrorism," *International Security,* Vol. 6, No. 4 (Spring), pp. 61-77.

Sterling, Claire (1981). *The Terror Network: The Secret War of International Terrorism.* New York: Holt, Rinehart, and Winston.

_____ (1984). *The Time of the Assassins.* New York: Holt, Rinehart, and Winston.

Stern, Jessica (2000). "Terrorist Motivations and Unconventional Weapons," in Peter R. Lavoy, Scott D. Sagan, and James Wirtz, eds., *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons.* Ithaca: Cornell University Press.

Stiglitz, Joseph E., and Linda J. Bilmes (2008). *The Three Trillion Dollar War: The True Cost of the Iraq Conflict.* New York: W.W. Norton & Company.

Suleyman, Mustafa, and Michael Bhaskar (2025). *The Coming Wave: AI, Power, and Our Future.* New York: Crown.

Taber. Robert (1965). *The War of the Flea: A Study of Guerrilla Warfare Theory and Practice.* New York: The Citadel Press.

Thompson, Nicholas (2009). "Inside the Apocalyptic Soviet Doomsday Machine." *Wired,* Vol. 17, No. 10 (October). Accessed at: https://www.wired.com.

Thornton, Thomas Perry (1964). "Terror as a Weapon of Political Agitation," in Harry Eckstein, ed., *Internal War: Problems and Approaches.* New York: The Free Press, pp. 71-99.

Vasiliev, A.M. and N.A. Zherlitsyna (2022). "The Evolution of al Qaeda: Between Regional Conflicts and a Globalist Perspective," *Herald of the Russian Academy of Sciences,* Vol. 92 (March), pp. 1240-1246. Accessed at: www.link.springer.com.

Verne, Jules (1879). *Les cinq cents millions de la Bégum* [the English translation shortened the title to *The Begum's Millions].* Paris: Pierre-Jules Hetzel. English translation by Stanford L. Luce. Middletown: Wesleyan University Press, 2005.

CHAPTER 3

Unconventional Terrorism: Future Trends in the Nuclear and Maritime Domains

Prof. Justin Hastings

Abstract

This chapter looks at the future trends in threats posed to NATO member states by terrorism in the unconventional maritime and nuclear domains. Analysis is based on the assumption that critical infrastructure in the maritime and nuclear domains will serve as both targets and force multipliers for terrorist attacks, and that emerging technologies, particularly drones and technologies embedded in maritime and nuclear infrastructure will create some new opportunities for violent non-state threats. Trends in terrorism writ large, and in the maritime and nuclear domains will expand the menu of viable terrorist targets, and enhance the disruption caused by attacks when they do occur. As terrorist networks decentralize and as states use violent non-state actors as proxies for attacks, the locations that are viable for terrorist attacks will expand. The nature of maritime infrastructure – ports, sea lanes, and global shipping networks, along with technological trends in shipping, will make attacking easier, and increase the disruption caused by well-placed terrorist attacks, while the expansion of nuclear infrastructure, the ready availability of radioactive sources, and the increasing importance of commercial facilities will make disruptive attacks more attractive for terrorists, but not necessarily deadlier. Recommended NATO member state responses revolve around developing a robust and nuanced response to nuclear and maritime terrorist threats, and maximizing the resilience of maritime and nuclear infrastructure.

1. Introduction

Unconventional terrorism can be broadly understood as terrorist attacks against targets, using methods, or in locations outside of the menu of typical terrorism. Where a conventional terrorist attack might involve a car bomb or a suicide attack against a civilian or political target in the middle of a city, unconventional terrorism might use materials and tools aside from explosives, guns, or knives, or might occur against targets that are not typical civilian, political, or military targets. While they do not exhaust the possibilities, nuclear terrorism and maritime terrorism are arguably two types of unconventional terrorism about which we can examine trends and challenges in the next fifteen years.

We define nuclear terrorism as attacks where terrorists attack or otherwise sabotage nuclear facilities or personnel, or attacks where terrorist use nuclear weapons or (less dramatically) nuclear materials or radioactive sources by themselves or in combination with high explosives as the attack vector (Allison, 2005, Ferguson and Potter, 2004).

Maritime terrorism can consist of terrorist attacks against maritime targets – both those on the water, whether seagoing ships or offshore platforms, and facilities connected with maritime trade and shipping lanes – naval bases, ports, and landside maritime cargo-handling facilities. Terrorists can seek to do damage to maritime targets, or to take the targets and personnel hostage as a means of achieving political and/or economic objectives. Terrorists can also use maritime transport or assets as a means of attacking land targets from the sea (Lehr, 2010, Ong, 2004, Richardson, 2004, Greenberg et al., 2006).

Unconventional terrorism is important because of two potential differences from conventional terrorism. First, although the probability that a given unconventional terrorist attack will occur tends to be low compared to the ambient threat posed by conventional terrorism (let alone stochastic political violence), if an unconventional attack does occur, it may do disproportionate damage or have disproportionate effects: an actual nuclear weapon detonation could kill tens of thousands, while a radioactive dispersal device could create psychological concern among the population, and cost significant amounts in cleanup. Second, the attack vector of unconventional terrorism can come from a direction that is not anticipated, or at least not particularly surveilled relative to conventional attacks. In the November 2008 Mumbai terrorist attacks that killed 166 people over multiple locations over several days, for example, the terrorists hijacked an Indian fishing vessel, allowing them to land in Mumbai directly from the Arabian Sea, with the attackers reportedly having links to Pakistan, and thus to catch security forces unaware (Rabasa et al., 2009).

This paper starts with the assumption that critical infrastructure in the maritime and nuclear domains will serve as both targets and force multipliers for terrorist attacks, and that those emerging technologies, particularly drones and technologies surrounding the operation of maritime and nuclear infrastructure will create some new opportunities for violent non-state threats. Trends in terrorism writ large, and in the maritime and nuclear domains will expand the menu of viable terrorist targets, enhance the disruption caused by attacks when they do occur. As terrorist networks decentralize and as states use violent non-state actors as proxies for attacks, the locations that are viable for terrorist attacks will expand. The nature of maritime infrastructure – ports, sea lanes, and global shipping networks, along with technological trends in shipping, will make attacking easier, and increase the disruption caused by well-placed terrorist attacks, while the expansion of nuclear infrastructure, the ready availability of radioactive sources, and the increasing

importance of commercial facilities will make disruptive attacks more attractive for terrorists, but not necessarily deadlier. Recommended NATO member state responses revolve around developing a robust and nuanced response to nuclear and maritime terrorist threats, and maximizing the resilience of maritime and nuclear infrastructure.

2. Core assumptions

The primary assumption of this assessment is that the future development and use of critical infrastructure is at the core of trends in the threats posed by unconventional terrorism, particularly nuclear and maritime terrorism. Attacking certain points of critical infrastructure will allow terrorists to maximize the damage they do, and *using* the critical infrastructure will ease the ability of terrorists to operate, and allow them to operate in new, perhaps unexpected ways. Both the nuclear domain and the maritime domain have such critical chokepoints: in the nuclear domain, the power plants and more specifically the areas containing fuel or waste, and reactors themselves, while generally well protected, can, if attacked or sabotage, have disproportionate effects not only on power provision, but also safety for relatively large areas downwind of the plant in the event of an atmospheric release.

In the maritime domain, ports and associated facilities are clear targets for terrorists, as are the means of transport – the seagoing ships themselves. Attacking either ports, ships, or offshore platforms can have deleterious safety and environmental consequences (such as oil spills), aside from the direct loss of life and economic damage. Because of the hub-and-spoke nature of global shipping networks' port infrastructure, with most global shipping being funneled to and transferred at massive transshipment ports, disrupting trade at those ports can have knock-on effects elsewhere. In addition, because of the geography of sea lines of communication globally, many shipping lanes (on the way to or from transshipment ports) pass through narrow seas surrounded on both sides by territory where state capacity is low. The Malacca Strait connecting the Indian Ocean and the South China Sea, the Bab al-Mandab between the Red Sea and the Arabian Sea, are both narrow shipping lanes that have come under attack from violent non-state actors on either side of the straits.

Both the nuclear and the maritime domain will see an intensification of the use of existing infrastructure, and an expansion of facilities and uses to new countries. This trend will be accompanied by emerging technologies that will ease or enable some unconventional terrorism strategies. In the nuclear domain, this would include an increase in the number of nuclear power plants around the world, and an increase in the number of countries with research reactors. Some countries will also develop other parts of the nuclear fuel cycle, including uranium and thorium mining, uranium processing, enrichment, fuel fabrication, reprocessing, and waste storage. Crucially, an assumption is that the ongoing development of less developed countries in the

Global South, including in medicine, value-added manufacturing, and mining, will lead to an increased number of facilities throughout the territory of an increased number of developing countries where radioactive sources may be present.

In the maritime domain, the number of seagoing ships will increase in the decades to come, and new import and export ports and transshipment ports will come online and expand their roles in global shipping. As with nuclear facilities, these ports will in some places expand to developing countries in the Global South with less state capacity. Ships themselves will be increasingly autonomous when using new technology, leading to fewer (or even no) crews on the ships.

1. Future trends and challenges

1.1. In terrorism

Two trends in terrorism are likely to change the calculus for nuclear and maritime terrorism in the next fifteen years. First, while states have always used non-state actors as proxies who can stage attacks with minimal investment from, and plausible deniability for the state (Byman, 2005, Byman and Kreps, 2010), the combination of terrorist groups with some amount of territorial control, strategic geographic location, and technological assistance and funding from states will exacerbate the ability of these groups to do damage to their chosen adversaries. A trend in the rise of ‘public-private partnerships’ such adversary states’ use of non-state proxies to attack or otherwise imperil nuclear and maritime targets, is likely to continue and increase in intensity over the time period under question (Allied Command Transformation 2023).

The Houthis’ ability to depress the volume of global shipping going through the Bab al-Mandab through intermittent cruise missile and drone attacks, and hijackings came about from a fortunate (for the Houthis) confluence of uncontested territorial control of Yemen territory immediately adjacent to the Bab al-Mandab, and cruise missiles and drone parts provided to the Houthis by Iran through dhow (a traditional Arabian sailing vessel) smuggling via the Arabian Sea (Bahadur, 2020).

Militant organisations with state support are clearly able to innovate. Upon the reignition of the conflict between Israel and Hezbollah in southern Lebanon in March 2026, for instance, Hezbollah began deploying small first-person view drones on fibre optic guide wires to bypass Israeli defences and attack Israeli forces (Unger and Durbin, 17 May 2026).

However, militant groups that do not receive state support can also, with sufficient space for adaptation and some amount of territorial control, adopt new technologies to increase the scale and scope of their attacks. For example, both sides

used drones in the 2017 Siege of Marawi in the Philippines. Similarly, the alliance of rebel groups fighting the junta in Myanmar's civil war has seen a rapid evolution in their capacity to import, build, and deploy drones for surveillance, reconnaissance, support, and offensive purposes in the course of the civil war (as have, to be fair, junta forces) (Naradichiantama, 9 May 2025).

Second, the focus in the immediate aftermath of 9/11 was on transnational terrorist groups, with organizational structures that spanned multiple countries, and generally easy movement of personnel, money, and to a lesser extent weapons across international boundaries (Cronin, 2002-2003). With the decline of Al-Qaeda, this model gave way to terrorist groups that, while they maintained a territorial basis, encouraged attacks in far locations via semi-autonomous cells or individuals inspired by, and sometimes instructed, by the core terrorist network. While DAESH was based primarily in Iraq and Syria, it encouraged (and then took credit for) attackers by its supporters, inspired by DAESH's success in the Middle East, throughout the world (Jasper and Moreland, 29 October 2016). It was a strategy that sacrificed command and control for reach.

As noted in Strategic Foresight Analysis 2023 (Allied Command Transformation 2023), decentralized terrorist networks are an excellent example of the rise of human networks as a factor in modern conflict. The idea of a structurally flat networked terrorist movement, with autonomous cells staging attacks with local sourcing of weapons and personnel, and with little more than loose coordination and generic training is also not new (Arquilla and Ronfeldt, 2001). Without significant external resources or training, terrorist attackers, whether as individuals or in cells, are likely to be able to carry out less sophisticated attacks than Al-Qaeda or DAESH were capable of in the past. However, because attackers, operating in or near their home countries, may have no organizational connection to larger international movements, and may be radicalized largely through passive consumption of ideological materials and social media, *where* they can attack is likely to change: radicalized, local, autonomous attackers who have largely gone under the radar of state law enforcement because of their lack of travel, structural ties or communication with outside organisations can attack in more places, and may use more creative means of attack. The spate of car and truck ramming attacks in Europe at the height of DAESH's influence, including one in Nice, France that killed over 80 people (Nesser et al., 2016), is an example of a campaign of autonomous, local attacks that is nevertheless claimed by an inspirational transnational terrorist movement.

1.2. Nuclear domain

The reliance of military capabilities on the commercial sector is relevant in both nuclear and maritime terrorism, as protecting strategic commercial assets becomes more important (Allied Command Transformation 2023), and those assets as targets

increase in interest to terrorist actors. In the nuclear area, the trend is toward more commercial targets. Although it has sputtered at times, the ‘Nuclear Renaissance’ (Stulberg and Fuhrmann, 2013) has resulted in an increasing number of new power plants coming online since the early 2000s and is seeing the construction of power plants and research reactors in countries that were previously largely devoid of a nuclear industry. As of 2025, Türkiye, as a bridge country between Asia and Europe, and Egypt in North Africa are constructing large power plants. In the Middle East, Saudi Arabia is constructing a research reactor with plans to build the full nuclear fuel cycle, including domestically sourced and enriched uranium. China is, as of 2025, building 25 new nuclear power plants with a power generation capacity of around 33 GWe (World Nuclear Association, 2025a).

NATO member states, largely in Eastern Europe, are also constructing or planning to construct new nuclear power plants: aside from Türkiye with its nuclear power plant under construction, Poland has taken decisive steps to construct two nuclear power plants (with four reactors among them) by 2036, while Romania plans to construct two additional reactors by 2032, and Slovakia is constructing one additional reactor. Sweden has changed its energy to a 100% fossil fuel-free electricity policy, allowing it to build new nuclear power plants. It currently plans to build two large power plants by 2035, and a number of SMRs by 2045. In North America, the United States recently commissioned two new nuclear reactors (the Vogtle reactors) and has set an aim to quadruple its use of nuclear power by 2050, while Canada is building four new small modular reactors of its own design (World Nuclear Association, 2025a). Perhaps more realistically, three nuclear reactors that were shut down have applied for permission to restart operations and receive new fuel, with the first slated to come online in 2028. These reactors were in some cases financed by private companies with an eye to providing more power for artificial intelligence data centres: Microsoft, for example, has financed the restart of Three Mile Island for this purpose (Mandler, 20 September 2024).

The expansion of nuclear power into more developing countries means that nuclear power will eventually be present in countries with greater political and economic instability, which is often accompanied by terrorist or other violent activity. Egypt, for example, which has both terrorist activity and relative political and economic instability, is pursuing a civil nuclear power plant as of 2025. Conventional wars in the territory of countries with nuclear facilities are no longer unheard of – Russia’s capture of Zaporizhzhia Nuclear Power Plant in Ukraine during the initial phase of its full-scale invasion of Ukraine has led to the first time a nuclear power plant has been attacked during a war, with fighting in the vicinity of the power, weapons staged inside the plant’s perimeter, and drone and missile attacks against plant buildings, including one of the reactor containment towers in the years since the occupation began (International Atomic Energy Agency, 9 September 2022). Similarly, in a sign that nuclear facilities

may be targets in conflicts, in May 2026, a drone reportedly hit an electrical generator outside the inner perimeter of the Barakah Nuclear Power Plant in the United Arab Emirates in the aftermath of the hot phase of the US-Iran war (Al Jazeera Staff, 17 May 2026). Likewise, given that Syria's Assad regime eventually lost control over significant parts of its territory by 2024, a facility widely reported to have been a nuclear reactor, allegedly constructed with North Korea's assistance, did not come under the control of terrorist groups during the Syrian Civil War, as it had reportedly been destroyed several years prior to the start of the civil war, reportedly by Israel (British Broadcasting Corporation, 22 March 2018).

1.2.1. Changing technology

While there is now a plethora of small modular reactor designs, and inevitably many or even most of these designs will not become reality, at least some small modular reactors are likely to be built during the time frame in question. Within NATO member states, small modular reactors are under development or under construction in the United States, Canada, the United Kingdom, Czechia, Romania, Poland, Norway, Sweden, and France (World Nuclear Association, 2025b). While some of the SMRs will be co-located with existing nuclear power plants (such as the Darlington project in Canada) (World Nuclear Association, 2025a), changing technology may lead to more sites, in less centrally located areas, that might attract terrorist interest. A proliferation of potential targets does not necessarily mean an increase in the risk of atmospheric release or meltdowns in the case of attack: small modular reactor designs are by and large designed to be passively cooled and shut down automatically in the event of a problem, thus minimizing the chances of a meltdown. With that said, their containment systems are also smaller than for larger nuclear reactors, and the land footprint around them for security purposes may also be smaller (although by no means small).

In addition, the long-term trend, likely to continue, is toward a greater use of radioactive sources in medical, mining, and other industrial sectors in more developing countries. The cross-border trade in radioactive sources is likely to intensify, with more countries with more lax regulatory controls trading in radioactive sources. The vast majority of radioactive source or nuclear materials trafficking incidents over the past thirty years – defined as incidents in which materials (whether held by unauthorized persons or not) were found to be outside of regulatory control -- have actually been from radiation or radioactive sources detected among scrap metal (James Martin Center for Nonproliferation Studies, 2023). Of the incidents where individuals are found with radioactive sources and nuclear materials out of regulatory control, a portion of them involve individuals who stole something from a facility without realizing the contents were radioactive. A smaller portion involve individuals knowingly stealing materials, for the purpose of later sale or use. Many, but not all, of these individuals are associated with the facilities from which they stole the materials, representing

insider threats (James Martin Center for Nonproliferation Studies, 2023). Increased use of radioactive sources may thus result not necessarily in more terrorist attacks, but a greater availability of sources out of regulatory control for those who wish to use them to do harm.

1.2.2. Changing terrorist threats

Nuclear terrorism has several vectors. Nuclear facilities may become targets – terrorists may attack the facilities in order to damage the facilities, including the reactor or any nuclear materials. Terrorists may also use nuclear materials or radioactive sources in their attacks, either in tandem with explosives (for the purposes of dispersing radiation) or by themselves. Attacks with fully constructed nuclear weapons are unlikely. The effect of these attacks can come through release of radiation, or a psychological or economic effect *because the facility attacked or the material used is nuclear*, which can cause panic and/or notoriety for the attacks, and lead to an expensive cleanup effort. In 2011 for example, a religiously motivated violent extremist group terrorist cell bombed the outside of an Indonesian nuclear facility west of Jakarta because they believed an explosion would set off a chain reactor that would cause a larger explosion and radiation atmospheric release (Detik News, 26 March 2011, Detik News, 27 April 2011, Viva News, 3 November 2011).

The disaggregated nature of terrorist networks (and therefore terrorist attacks) will likely lead to a changing menu of potential targets, as terrorists plot attacks without detailed direction from central command nodes. While the overall capabilities of individual terrorists are unlikely to increase in the face of an absence of centralized training and indoctrination, an increase in the number of nuclear facilities will increase the potential locations that could be attacked (if doing very little damage). The physical damage that terrorist attackers will be able to do to nuclear facilities is likely to be small; the propaganda value of attacking a nuclear facility (and thus the reason to target such a facility) may be bigger.

The advent of drones in offensive acts even by non-state actors – even simple ones that can drop explosives and – will allow capable terrorists to threaten facilities that they would not otherwise be able to reach. Anti-drone technology will continue to evolve, but will be difficult to implement at all times in all locations, particularly in civilian areas outside conflict zones where equipment to detect and take down drones is not generally installed. While large-scale damage to nuclear facilities that releases radioactivity is unlikely, a campaign of harassment via drones against nuclear facilities and other energy-related or research facilities can have disruptive effects – the 2025 appearances of drones around airports in countries in Western Europe, suspected to be drones launched by Russian operatives, either from ships in

the Baltic Sea, or provocateurs on the ground in the countries (Associated Press, 6 November 2025), are an example of the disruptive effects even non-lethal drones can have when they come within the vicinity of sensitive critical infrastructure. Indeed, three drones were detected near a nuclear power plant in Belgium in November 2025 (Reuters, 10 November 2025).

The increase in the availability of radioactive sources and even spent fuel in many developing countries may provide more sources and opportunities for theft by terrorists. In general, very few radioactive source or even nuclear materials trafficking incidents have been related to terrorist attacks. Situations in which terrorist groups did attempt to acquire radioactive sources for dirty bomb attacks have often involved attempting to steal radioactive sources from industrial sites or extract radioactive sources from consumer products. One religiously motivated violent extremist group terrorist group in Indonesia in 2017 attempted to build radiation dispersal devices (‘dirty bombs’) by extracting thorium from camping lamps and materials from electronic waste that had been imported into Indonesia (BAPETEN, 27 September 2017). However, the availability of radioactive sources in more locations will provide opportunities for new kinds of terrorist attacks. Terrorists seeking radioactive sources need to be motivated but not necessarily particularly capable. In Indonesia, for instance, a large portion of radioactive sources that were lost to theft were due to mishandling by operators, or simple theft from vehicles and facilities (Kompas Online, 26 February 2006). The relatively easy access to radioactive sources will provide some support for interested terrorists.

Even without adding an explosive element, contaminated materials, which are a large position of radioactive sources out of regulatory control, can have disproportionate effects relative to their scale. A likely import of scrap metal containing cesium-137 into Indonesia in 2025, and the subsequent exposure resulted in a number of hospitalizations, the relocation of community members nearby, the decontamination of 22 facilities across the entire area of the affected industrial estate, and the recall of frozen shrimp exported to Walmart stores in the United States (Caldwell, 9 October 2025).

1.3. Maritime domain

Maritime terrorism’s targets become more strategically important as trade routes and supply chains becomes a priority for both states and private actors. The maritime domain is perhaps the greatest example of the global commons, the exploitation and protection of which will require improvements in range and readiness of military capabilities, as well as increased reliance on commercial assets (Allied Command Transformation, 2023). Nearly all global shipping is, for example, run by commercial providers. More generally, the intensification of the use of sea lines of communication and transshipment ports – an increase in the number of ships and

TEUs moving through ports and sea lanes – is a likely trend, conditional on an increase in global (and regional) trade over the next twenty years. Transshipment port intensification will primarily affect ports in East Asia, the Middle East, and Europe (goods shipped from East Asia to the United States generally go directly). NATO member states and their militaries are often reliant on the smooth functioning of these private-led maritime shipping networks.

As developing countries become more tightly integrated into the global economy, their ports will also increase in business, and the benefits to a terrorist group of attacking previously marginal ports, or shipping transiting to or from those ports, will likely increase. Multinational companies will move in to buy the ports or bid for their operation as a means of diversifying away from dependence on transshipment ports. The Tuas port of Singapore, for instance, is not physically capable of handling more than 65 million TEUs per year with its expansion (which is not expected until the 2040s). Once that limit is reached, the owner of the port, PSA, will begin sending transshipments through other ports in which it has bought interests. PSA has an operation contract for the port of Gwadar, and an ownership share in the port of Surabaya (PSA Singapore, 2025, Lloyds List, 7 Feb 2007).

A trend in the maritime domain that is seemingly orthogonal to terrorism but is nonetheless important in understanding the changing maritime terrorist threat is the decrease in state compliance with international norms on maritime security safety, and regulations on shipping, a trend that is likely to continue as the global order becomes subject to contestation by emerging powers and states unsatisfied with the order as it stands. This decline in compliance has come as a result of several factors. First, the United Nations sanctions regime has begun to fray – sanctions against Iran, North Korea, and other countries are undermined not only by the maritime assets (ships, companies, and personnel) owned by the sanctioned countries, but also by companies operating out of third countries (Hastings, May 2022, Hastings, 2022). Sanctions enforcement against North Korea, for instance, has dissipated in China, and has been entirely repudiated by Russia. The result is that both states and private companies have experienced less difficulty in evading sanctions. Second, war-related autonomous sanctions against some countries have led to situations in which both the targeted countries and their partners cooperate in ignoring the sanctions. China and India's continued purchase of oil from Russia in the face of European Union and United States sanctions is an example.

In practical terms, because of these burgeoning sanctions evasion networks, there now exist an ecosystem of individuals, companies, ports, and ships which have become well practiced in setting up networks and front companies, providing services for shadowy companies, falsifying transactions and insurance, registering ships in weak regulatory environments, and using tactics such as Automatic Identification System spoofing, that make it more difficult for them to be detected by the law

enforcement of other countries (see, for example, (C4ADS, 23 April 2020). These networks are largely but not totally private, and are willing to work for multiple countries and private actors – in July 2024, for instance, a ship, the *Ceres 1,* collided with another ship in the South China Sea east of Singapore. The *Ceres 1* had been involved in transferring both Iranian and Russian oil to ships destined for China at various points in the previous year, and had turned off its AIS for periods of time (apparently) during these transfers (Koh, 29 July 2024).

Third, the dynamics of maritime boundary disputes, particularly in Asia, have encouraged states to use (and therefore supply and empower) non-state and quasi-state assets to defend their sovereignty claims and the push the bounds of armed conflict into a gray zone. China in particular has equipped and deputized maritime militias and civilian fishing vessels to exploit fisheries and show the flag throughout the area it claims in the South China Sea. At times these vessels work in tandem with Chinese Coast Guard and even the PLA Navy to engage in aggressive but non-kinetic activities – swarming other vessels, ramming, spraying them with water, and the like. Other countries have likewise used quasi-state and non-state actors to push their claims, such as Vietnam and the Philippines encouraging their fishing fleets to fish in the areas they claim (Green et al., 2017, Morris, 2019, Dutton, 2022).

1.3.1. Changing technology

Changing technologies in the maritime domain are likely to influence the points of vulnerability of aspects of maritime shipping industry to terrorist attack, and the interest and ability of terrorists to attack different points of the maritime supply chain.

The requirement to use an Automated Identification System signal (which broadcasts the name, flag country, origin, destination, speed, heading, and ship type, among other information) for essentially any oceangoing ship over minimal tonnage means that potential targets have become easier for terrorists (or pirates) to track. At the same time, the *lack* of use of AIS by some ships as they seek to avoid being tracked – whether because they are engaged in smuggling, or are part of the shadow fleets that allow countries like Russia, Iran, and North Korea to evade United Nations and autonomous sanctions (Brooks and Harris, 27 February 2025) -- creates safety hazards in terms of potential ship collisions, particularly at inopportune times. Two ships, for example, collided in the Persian Gulf during a period of heightened tensions surrounding the Twelve Day War in 2025. One was reportedly a shadow tanker without insurance (Sellers, 17 June 2025).

The increasing automation of shipping also increases vulnerability to some threats. Given that sailors are a cost centre for shipowners, the global shipping industry has long sought to decrease the number of personnel on board ships through

the use of automation. Large oil tankers and container ships now average 20-25 personnel on board, down from 30-40 during the Cold War. Conditional on the size, freeboard, and speed of a ship, fewer crew on board ships makes ships easier for pirates and terrorists to hijack or attack.

The next fifteen years could potentially even see the advent of cargo ship drones without any personnel at all. In 2019, a drone, Saildrone, crossed the Atlantic between Bermuda and the United Kingdom twice, marking the first double cross-Atlantic crossing by an unmanned vessel (Saildrone, n.d.). Since then, sea drone capabilities have only increased, and costs have come down. Uncrewed cargo sea drones will present a tempting target for maritime-capable terrorist attackers. While remote operators will certainly have the ability to take evasive action or deny attackers the ability to pilot the drone, preventing damage to the drone by erstwhile attackers will be somewhat more difficult.

Drone ships may also become weapons themselves. Connectivity and automation will also likely ease the ability of both state and non-state actors to create and direct submerged and semi-submerged drone vessels. Past maritime attacks directly against ships have run into the problem of placing individual terrorists adjacent to or on the target ships: before the successful attacks on the *USS Cole* and *MV* Al-Qaeda had several plots that ran aground (no pun intended) because of the need to get people close to the target. One explosive-laden boat sank before reaching the target because it was too heavy for the load; another plot based on scuba diving Al-Qaeda operatives placing explosives against ships from below also failed (Greenberg et al., 2006, Lorenz, 2007). The explosives-filled boats created by the Tamil Tigers during the Sri Lankan civil war that were successful during the war in sinking or disabling a third of the Sri Lankan navy were directly piloted by suicide attackers (Sridhar, 2008).

Unmanned attack capabilities at sea by non-state and quasi-state actors are also progressing steadily. The Houthis in Yemen have, since 2016, perpetrated a sophisticated campaign of disruption and active attacks on shipping going to and from ports in the Red Sea, passing through the Red Sea and the Gulf of Aden. This campaign has included not only sea mines in ports in Yemen, and anti-ship missiles and GPS-guided attack airborne drones, but also unmanned attack sea drones fashioned out of skiffs, and eventually unmanned undersea vessels as well. The sea drones were themselves apparently given greater attack capacity and range through the use of a mother ship that towed the drones closer to their targets in a Saudi port, and the Houthis have attempted small swarms of attack sea drones against target vessels at times. Notably, while the anti-ship missiles used in the Houthis' post-October 7 campaign against Israel-linked shipping in the Red Sea and Gulf of Aden were smuggled in parts from Iran, and put together in Houthi-controlled territory, the sea drones have been largely designed by Houthis, and put together in Houthi

factories using commercially available parts (Panel of Experts, 25 January 2021, Panel of Experts, 26 January 2022, Panel o fExperts, 11 October 2024).

1.3.2. Changing terrorist threats

Traditionally, the maritime domain was seen as a poor theatre of operations for terrorist groups: as terrorists are largely land-based non-state groups, attacking sea-based targets was seen as outside the capabilities of many terrorist groups (or required them to develop capabilities to operate on sea that they did not previously have), and maritime targets themselves were viewed as poor targets for terrorist purposes: they were potentially far from land, populations that could be damaged, and media that could visually show the effects of the attack (Asal et al., 2019, Asal and Hastings, 2015). With the advent of social media and Internet connectivity virtually anywhere in the world, the menu of potential visually arresting terror targets has expanded outside of the central business districts of major cities.

It is also the maritime domain where terrorist groups are likely to be empowered and supplied by states seeking proxy actors. Where one of the past constraints on maritime terrorism was the limited maritime capacity and knowledge of terrorist groups, such that only relatively capable and longstanding groups with some amount of territorial control to use as safe havens tended to try major maritime attacks, states providing boats, drones, cruise missiles (and to a lesser extent ballistic missiles) to terrorist groups, as well as training in how to use them, are likely to result in groups with more capability being able to attack ships in locations that were previously out of reach. The breakdown in international norms of behaviour in international waters, but especially contested waters, means that states may seek out means of enabling attacks on adversaries' ships and ports without escalating to interstate conflict.

States using terrorist groups as proxies, and terrorist groups using locally placed individuals as attackers extends their reach, and provides capabilities that the actual attackers would not otherwise have. On land, this has already happened. The practice, by both Russia and Ukraine, in the current war, of bribing locals to engage in acts of sabotage of targets that would otherwise be unreachable using more conventional weapons, is a case in point (Miller, 30 June 2025). Highly automated commercial ships will be more vulnerable to attack by determined terrorists, and the rise of privately owned semi-submerged drones that can be used in attacks will widen the menu of potential targets and locations that can be attacked, particularly given that commercial ports that are otherwise at peace are unlikely to have the anti-drone measures common in the Black Sea during the Russia-Ukraine War.

More crowded, narrow shipping lanes, the expansion of logistics networks to new ports, and the intensification of the use of ports in developing countries will ease terrorist groups' ability to target both warships and commercial ships from land,

and will also heighten the knock-on effects of attacks at critical chokepoints. Attacks at critical chokepoints will continue to have outsize effects, as seen, for example in the effects of the Houthis' post-October 7 missile, drone, and hijacking campaign against Israel-linked ships passing through the Bab al-Mandab. The rise of shadow fleets with old ships with poor safety records, questionable ownership, falsified insurance, and intermittent or no use of AIS provides well-resourced terrorists with a potential playbook, or even a supply of ships that could be attacked, sabotaged, or repurposed for either logistical support or violent attacks. Disabled ships adrift in crowded shipping lanes or ports, or ships hijacked by terrorists and deliberately crashed into ports or other ships may present safety and security hazards.

2. Recommendations

- NATO states and partner countries are recommended to improve the security culture not only of large nuclear facilities and commercial ports, but also industrial sites containing radioactive sources, and port facilities in emerging countries where the vulnerability to terrorist sabotage, theft, or attack likely exceeds their attention to security from those threats.
- Continued development of anti-drone technology will happen regardless of the terrorist threat posed, but the placement of anti-drone measures is proposed to be extended to new and existing nuclear facilities, as well as ports. NATO member states and partner countries with the means to do so could also consider providing aid for these technologies to be installed and maintained in critical infrastructure points in developing countries.
- Because much of the damage and disruption likely to arise from unconventional terrorism is actually derived from the governments' response and public panic, it would behove governments to tailor responses to attacks and threats in ways that minimize disruption to daily life, and to conduct public education programs that minimize psychological effects of radiological attacks in particular.
- Because much of the vulnerability of countries to unconventional terrorism comes from the multiplying effects of attacks on critical infrastructural nodes, counterterrorism programs might as part of larger security programs focus on increasing the resilience of physical supply chains in the maritime domain.
- As adversary states encourage or supply violent non-state actors with the tools, capacity, and weapons to attack both nuclear facilities and maritime targets – ports, ships, and pipelines – counterterrorist policy might usefully focus on cutting off supply from states to terrorist actors. While this is obvious, in the maritime domain, this would involve more aggressive enforcement of regulations against shadow fleet vessels where international law allows, more aggressive action against ships suspected of violating United Nations sanctions, and more aggressive responses to gray zone tactics by putative non-state actors.

References

Al Jazeera Staff. 17 May 2026. Drone strike sparks fire on perimeter of UAE's Barakah nuclear power plant. *Al Jazeera*.

Allied Command Transformation. *Strategic Foresight Analysis 2023*. Norfolk, VA: Allied Command Transformation, North Atlantic Treaty Organization.

Allison, G. 2005. *Nuclear Terrorism: The Ultimate Preventable Catastrophe,* New York, Macmillan.

Arquilla, J. & Ronfeldt, D. (eds.) 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy,* Santa Monica: RAND.

Asal, V. & Hastings, J. V. 2015. When Terrorism Goes to Sea: Terrorist Organizations and the Move to Maritime Targets. *Terrorism and Political Violence,* 27**,** 722-740.

Asal, V., Hastings, J. V. & Rethemeyer, K. 2019. Maritime Insurgency. Sydney and Albany: University of Sydney and the University at Albany, State University of New York.

Associated Press 6 November 2025. As Russian drone incursions rattle Europe, Poland and Romania deploy a new defensive system. *Australian Broadcasting Corporation*.

Bahadur, J. 2020. Snapping back against Iran: The case of the *Al Bari 2* and the UN arms embargo. *Policy Brief.* Geneva: Global Initiative against Transnational Organized Crime.

Bapeten 27 September 2017. Bapeten Sebut Teror Bandung Nyaris Mengarah ke Serangan Nuklir. Jakarta: Bapeten.

BBC 22 March 2018. Israel admits striking suspected Syrian nuclear reactor in 2007. *British Broadcasting Corporation*.

Brooks, R. & Harris, B. 27 February 2025. Where did Russia's shadow fleet come from? Washington, DC: Brookings Institution.

Byman, D. 2005. *Deadly Connections: States that Sponsor Terrorism,* Cambridge, UK, Cambridge University Press.

Byman, D. & Kreps, S. E. 2010. Agents of Destruction? Applying Principal- Agent Analysis to State-Sponsored Terrorism. *International Studies Perspectives,* 11**,** 1-18.

C4ADS 23 April 2020. A Hull in their Story: Satellite imagery, AIS, and the Ships Secretly Transporting Iranian Gas to China. *Commentary.* C4ADS.

Caldwell, I. 9 October 2025. 'Radioactive' shrimp crisis: Indonesia grapples with contaminated industrial zone. *The Guardian*.

Cronin, A. K. 2002-2003. Behind the Curve: Globalization and International Terrorism. *International Security,* 27**,** 30-58.

Detik News 26 March 2011. ‘Bom' di Jl Raya Puspiptek Dilempar dari Mobil Avanza. *Detik News*.

Detik News 27 April 2011. Daftar 17 Tersangka Bom Buku & Serpong. *Detik News*.

Dutton, P. A. 2022. Conceptualizing China's Maritime Gray Zone Operations. *Maritime Gray Zone Operations.* Routledge.

Ferguson, C. D. & Potter, W. C. 2004. The Four Faces of Nuclear Terrorism. Monterey, CA: Center for Nonproliferation Studies, Monterey Institute of International Studies.

Green, M., Hicks, K., Cooper, Z., Schaus, J. & Douglas, J. 2017. Countering coercion in maritime Asia: The theory and practice of gray zone deterrence. Washington, DC: Center for Strategic and International Studies.

Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I. & Ortiz, D. S. 2006. *Maritime Terrorism: Risk and Liability,* Santa Monica, CA, RAND Corporation.

Hastings, J. V. 2022. North Korean trade network adaptation strategies under sanctions: Implications for denuclearization. *Asia and the Global Economy,* 2**,** 100031.

Hastings, J. V. May 2022. Maritime Crime Associated with Weapons of Mass Destruction Proliferation and Sanctions Evasion. Colombo: Global Maritime Crime Programme, United Nations Office on Drugs and Crime.

IAEA. 9 September 2022. Nuclear Safety, Security and Safeguards in Ukraine International Atomic Energy Agency.

Jasper, S. & Moreland, S. 29 October 2016. ISIS: An Adaptive Hybrid Threat in Transition. *Small Wars Journal*.

Koh, F. 29 July 2024. CNA Explains: What we know about a hit-and-run off Pedra Branca involving an alleged ‘dark ship’. *Channel News Asia*.

Lehr, P. 2010. Maritime Terrorism: Locations, Actors, and Capabilities. *In:* Peter Lehr, S. B., Rupert Hebert Burns (ed.) *Lloyd's MIU Handbook of Maritime Security.* Boca Raton, FL: CRC Press.

Lloyds List 7 Feb 2007. PSA signs 40-year commitment to operate Gwadar deepsea terminal. *Lloyd’s List*.

Lorenz, A. J. 2007. Al Qaeda's Maritime Threat. Ramat Hasharon, Israel: Intelligence and Terrorism Information Center at the Israel Intelligence Heritage & Commemoration Center (IICC).

Mandler, C. 20 September 2024. *Three Mile Island nuclear plant will reopen to power Microsoft data centers* [Online]. National Public Radio. Available: https://www.npr.org/2024/09/20/nx-s1-5120581/three-mile-island-nuclear-power-plant-microsoft-ai [Accessed].

Miller, C. 30 June 2025. Russia grooms Ukrainian teens as spies and saboteurs. *Financial Times*.

Morris, L. J. 2019. Gray zone challenges in the East and South China sea. *Maritime Issues,* 7.

Naradichiantama, D. 9 May 2025. The shifting landscape of Southeast Asian UAV programmes. *Online Analysis.* London: International Institute for Strategic Studies.

Nesser, P., Stenersen, A. & Oftedal, E. 2016. Jihadi terrorism in Europe: The IS-effect. *Perspectives on terrorism,* 10**,** 3-24.

Ong, G. G. 2004. 'Ships Can Be Dangerous Too': Coupling Piracy and Maritime Terrorism in Southeast Asia's Maritime Security Framework. Singapore: Institute of Southeast Asian Studies.

Kompas Online 26 February 2006. Tahun 2008 Minimal Terjadi 7 Kecelakaan Nuklir di Indonesia. *KOMPAS*.

Panel of Experts 11 October 2024. Final report of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140 (2014). New York City: United Nations Security Council.

Panel of Experts 25 January 2021. Final report of the Panel of Experts on Yemen. New York City: United Nations Security Council.

Panel of Experts 26 January 2022. Final report of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140 (2014). New York City: United Nations Security Council.

PSA Singapore 2025. *Our Business: Making Global Trade Possible* [Online]. Singapore: PSA Singapore. Available: https://www.singaporepsa.com/our-business/port/ [Accessed].

Rabasa, A., Blackwill, R. D., Chalk, P., Cragin, K., Fair, C. C., Jackson, B. A., Jenkins, B. M., Jones, S. G., Shestak, N. & Tellis, A. J. 2009. The Lessons of Mumbai. Santa Monica, CA: RAND Corporation.

Reuters. 10 November 2025. Three drones detected over Belgium’s Doel nuclear power plant. *Al Arabiya English*.

Richardson, M. 2004. *A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction,* Singapore, Institute of Southeast Asian Studies.

Saildrone. n.d.: Saildrone. Available: https://www.saildrone.com/missions/atlantic-crossing [Accessed].

Sellers, M. 17 June 2025. *Collision in the Gulf sparks renewed concern over shadow fleet, war risk exposure* [Online]. Insurance Business. Available: https://www.insurancebusinessmag.com/us/news/marine/collision-in-the-gulf-sparks-renewed-concern-over-shadow-fleet-war-risk-exposure-539412.aspx [Accessed].

Sridhar, R. 2008. Maritime Terrorism Capability of the Sea Tigers of Sri Lanka. *In:* PARASHAR, S. (ed.) *Maritime Counter-Terrorism: A Pan-Asian Perspective.* New Delhi: Dorsey Kindersley India.

James Martin Center for Nonproliferation Studies 2023. CNS Global Incidents and Trafficking Database. Washington, DC: Nuclear Threat Initiative.

Stulberg, A. & Fuhrmann, M. (eds.) 2013. *The Nuclear Renaissance and International Security,* Stanford, CA: Stanford University Press.

Unger, L. & Durbin, A. 17 May 2026. Hezbollah drone strike videos show evolving tactics against Israel. *British Broadcasting Corporation.*

Viva News 3 November 2011. Dikira Simpan Nuklir, Puspitek Target Bom. *Viva News*.

World Nuclear Association. 2025a. *Information Library* [Online]. World Nuclear Association. Available: https://world-nuclear.org/information-library [Accessed].

World Nuclear Association. 2025b. *Small Modular Reactor (SMR) Global Tracker* [Online]. World Nuclear Association. Available: https://world-nuclear.org/information-library/current-and-future-generation/small-modular-reactor-smr-global-tracker [Accessed].

CHAPTER 4

Transnational Terrorism in Africa: Mapping A New Role for NATO on the Continent

Dr. Christina Schori Liang

Abstract

This chapter examines the evolving nature of transnational terrorism in Africa. It traces the historical evolution of terrorism across the continent. It begins by describing how local insurgencies have become embedded within broader transnational networks that exploit weak governance, porous borders, and regional instability. Contemporary terrorism in Africa cannot be understood in isolation but must be viewed within the interconnected dynamics of protracted conflict, demographic pressures, economic marginalization, and the growing impacts of climate change. These structural drivers reinforce one another, creating an environment in which violent extremist organizations can expand, adapt, and sustain their operations. At the same time, emerging technologies are reshaping the threat landscape in Africa especially drones, satellite internet services and encrypted communications, which are expanding the operational capabilities of terrorist organizations while simultaneously presenting new opportunities for counterterrorism operations. Durable security outcomes depend on African-led solutions, underpinned by African leadership. Long-term success in countering transnational terrorism depends upon strengthening African institutions and regional mechanisms, particularly the African Union (AU) and the Economic Community of West African States (ECOWAS), while reinforcing complementary partnerships with NATO and the United Nations. NATO's greatest contribution to addressing security challenges in Africa lies not in direct military intervention, but in strengthening the capabilities and resilience of African partners themselves.

Introduction

Africa's growing strategic importance makes the continent central to contemporary discussions of international security. By 2050, Africa is projected to account for approximately 25 percent of the world's population, while 12 of the 20 fastest-growing economies in 2025 are located on the continent. Yet alongside these opportunities, Africa faces significant security challenges, foremost among them the rapid expansion of violent extremism and terrorism. The spread of terrorist and militant groups across the Sahel, the Lake Chad Basin, the Horn of Africa as well as parts of Southern Africa has transformed terrorism from a largely localized concern into a transnational threat with implications extending well beyond the continent. These

dynamics are increasingly linked to broader challenges including burgeoning climate change, irregular migration, maritime insecurity, transnational organized crime, and intensifying geopolitical competition. As a result, instability in Africa has become closely intertwined with European, transatlantic, and global security interests.

The scale of this challenge is reflected in recent trends. Africa accounted for more than 51 percent of global terrorism-related deaths in 2024, making it the region most affected by extremist violence worldwide. According to the Global Terrorism Index 2026, terrorism-related deaths in the Sahel have increased tenfold since 2007, establishing the region as one of the principal epicentres of global terrorism. Four West African states now rank among the countries most severely affected by terrorist activity. This deterioration is not the result of a single crisis or temporary escalation. Rather, it reflects the cumulative impact of rapid demographic growth, widespread governance failures, and chronic insecurity compounded by the environmental pressures due to climate change. The growing proliferation of modern weaponry and the adaptive capacity of violent non-state actors alongside the erosion of traditional mechanisms for conflict resolution have increased insecurity across the continent.

Africa has become increasingly important to NATO because instability on the continent is now seen as directly connected to European and transatlantic security interests (Šikl, 2021). Rather than being viewed as geographically distant, regions such as North Africa, the Sahel, and the Horn of Africa are increasingly considered part of NATO's wider "southern neighborhood," where insecurity can spill over into Europe through migration pressures, organized crime, and regional conflicts. As a result, instability in Africa came to be viewed not as a localized issue, but as a potential source of transnational threats capable of affecting NATO member states directly. Despite the scale and strategic significance of these developments, NATO's role in Africa remains conceptually ambiguous, politically contested, and strategically underdeveloped. This chapter hopes to shed some light on what should be NATO's objectives in Africa.

However, before there is any meaningful discussion of NATO's future role on the continent, there must be a clear diagnosis of how Africa became the new center of terrorist violence and what are the structural conditions in Africa's that are driving the expansion of violence by terrorist groups, insurgent groups and private military companies.

The global center of terrorist violence has progressively shifted from the Middle East to Africa due to a combination of factors which include structural conditions that lead to local fragility. Following the sustained counterterrorism pressure in Iraq and Syria, particularly the military degradation of DAESH and Al-Qaeda leadership networks, extremist organizations adapted by relocating and embedding themselves

in weaker and more fragmented governance environments (Dowd and Raleigh, 2013; Pérouse de Montclos, 2014). Africa—especially the Sahel, Lake Chad Basin, and Horn of Africa—has proven highly conducive to this diffusion due to weak state capacity, porous borders and recurring political instability (UNDP, 2023; ACLED, 2024). As a result, global religiously motivated violent extremist (RMVE) networks, such as al-Shabaab, Boko Haram, and Islamic State Sahel Province (ISSP) have become increasingly decentralized and locally rooted, transforming Africa into the primary theatre of contemporary terrorist activity.

The Evolution of African Terrorist Groups

Africa's current concentration of terrorist groups is largely rooted in long-term structural and historical conditions rather than a single cause. These include the crisis of the postcolonial state. Many regions inherited weak state institutions and contested borders following decolonization in the mid-20th century, which in some cases contributed to fragile governance and limited state presence in remote areas. These gaps created environments where armed groups could operate with relative freedom.

Africa is home to about 20 percent of the world's population but accounts for approximately five percent of global economic activity (World Bank, 2024). Africa's relatively low share of global economic output is rooted in its historical development. During colonial rule, many economies were structured to extract raw materials rather than build diversified industries, leaving behind limited industrial bases and infrastructure designed mainly for export rather than internal growth (Rodney, 2018). After independence, countries inherited these structural constraints along with borders and institutions that were not always well-suited for stable governance, contributing in some cases to political instability, conflict, and inconsistent economic policies that discouraged investment and long-term planning (Acemoglu and Robinson, 2012).

Research by the Soufan Center argues that many governments across the Sahel and parts of Sub-Saharan Africa struggle to maintain effective control over their territories, particularly in rural and border regions where extremist violence, organized crime, and communal conflict are prevalent. Weak institutions, corruption, and poor delivery of public services have reduced confidence in civilian governments, while security forces are often underfunded and poorly trained, and are considered to be largely ineffective by their local populations (The Soufan Center, 2024).

In several cases, governments have been accused of concentrating power among narrow political elites while failing to address local grievances or provide meaningful economic opportunities. This has weakened the social contract between states and citizens, increasing public frustration and creating conditions where military coups can gain domestic support, particularly when elected governments are seen as corrupt or incapable of addressing insecurity (ICG, 2024). In order to find the best

responses to the growing threat of terrorism and insurgency in Africa it is important to focus on the evolution of terrorism especially as it has evolved in Africa in general and in West Africa in particular.

Evolution of Terrorism in West Africa (2000–2026)

The evolution of terrorism between 2000 and 2010 can best be characterized as a localized and fragmented phase of violent extremism in West Africa. During this period, militant activity remained relatively limited in both scale and geographic reach. Groups such as the Salafist Group for Preaching and Combat (GSPC), the precursor to Al-Qaeda in the Islamic Maghreb (AQIM), operated primarily through dispersed cells conducting isolated attacks in remote border areas across the Sahara-Sahel region. These operations were generally opportunistic, low in sophistication, and constrained by limited logistical capabilities, resulting in comparatively low casualty figures and minimal territorial control. Militant violence during this phase remained episodic rather than sustained, and despite weak governance in peripheral regions, state authority broadly remained intact across most national territories (Thurston, 2020; ICG, 2013).

The period from 2011 to 2015 marked a decisive expansion phase driven by regional geopolitical shocks, state collapse, and the proliferation of weapons and fighters following the collapse of Libya in 2011. NATO's intervention in Libya is frequently described as a short-term operational success but a long-term strategic failure. While the intervention achieved its immediate objective of protecting civilians and facilitating the removal of Muammar Gaddafi, insufficient planning for post-conflict stabilization and institutional reconstruction created a significant governance vacuum after the regime's collapse (UNSC, 2011).

In the absence of a functioning central authority, Libya fragmented into competing militia-controlled territories. Many of these militias had initially received support during the intervention but were never effectively disarmed afterwards. The subsequent spread of weapons and fighters across the Sahel, combined with longstanding governance weaknesses, directly contributed to the 2012 Mali crisis, during which northern Mali fell under the control of AQIM-linked organizations including Ansar Dine and the Movement for Unity and Jihad in West Africa (MUJAO) (Lecocq et al., 2013).

At the same time, Boko Haram underwent rapid transformation in northeastern Nigeria, evolving from a relatively localized insurgent movement into a major violent extremist organization capable of controlling territory and conducting large-scale attacks against civilian and military targets alike (Pérouse de Montclos, 2014). Compared with the preceding decade, this phase was characterized by sustained territorial occupation, higher casualty rates, and the emergence of insurgent governance structures across contested areas.

From 2015 onwards, terrorism in West Africa entered what can be described as a dispersed networks phase, characterized by the fragmentation of earlier organizations and the emergence of more decentralized and adaptive militant ecosystems. Transnational extremist groups increasingly embedded themselves within local political, ethnic, and economic grievances rather than operating solely as externally imposed ideological movements. Organizations such as al-Shabaab, Boko Haram, and DAESH-affiliated groups adapted their strategies to local conditions, exploiting governance vacuums, state fragility, and social exclusion to deepen their influence (Thurston, 2020; Walther and Christopoulos, 2015).

In many rural and peripheral regions, limited state presence, corruption, uneven development, and abusive security practices created permissive environments in which insurgent organizations were able to provide rudimentary governance, dispute resolution, and protection services. Through these mechanisms, extremist groups acquired varying degrees of local legitimacy and support (Dowd and Raleigh, 2013). This process of localization transformed many originally transnational organizations into hybrid actors that were simultaneously globally connected and locally embedded, significantly complicating counterterrorism responses (UNDP, 2023).

Key challenge: Transnational Organized Crime

By the late 2010s, the Sahel had emerged as growing center of terrorism, accounting for an increasingly large share of terrorism-related deaths worldwide. One of the defining features of this period was the growing convergence between terrorism and organized crime. Armed groups evolved beyond purely ideological insurgencies and developed hybrid economic systems based on trafficking networks involving drugs, weapons, fuel, and human smuggling. In countries such as Mali, terrorist organizations became deeply integrated into local economies and governance systems through taxation, control of trade corridors, protection rackets and even marriage. These criminal-terrorist linkages significantly enhanced the resilience and financial autonomy of militant groups, enabling them to sustain operations despite prolonged counterterrorism pressure (Institute for Economics & Peace, 2025). Consequently, distinctions between insurgency, organized crime, and political violence became increasingly blurred. The widening threat of terrorist groups led to a period of external military interventions.

Key Challenges: External Military Actors

European states, particularly France, initially led large-scale counterterrorism and stabilization operations in Mali and across the wider Sahel. Military Operations such as Operation Barkhane achieved a number of tactical successes against terrorist leaders and militant infrastructure. However, these gains proved strategically unsustainable due to recurring military coups, deteriorating political legitimacy,

growing anti-Western sentiment, and intensifying geopolitical competition involving actors such as Russia (International Crisis Group, 2023). As relations between Sahelian governments and Western partners deteriorated, European military forces were progressively compelled to withdraw or substantially reduce their presence.

The spread of terrorism across the Sahel further exposed the structural limitations of post-9/11 Western counterterrorism models which largely relied on assumptions that terrorism could be defeated primarily through military force, kinetic operations, and state-centric security partnerships. However, multiple experiences in Afghanistan, Iraq, Libya, and the Sahel demonstrated that military intervention alone was insufficient to address the complex security terrain fraught by underlying governance crises, political exclusion, and socioeconomic inequalities that sustain insurgencies (Charbonneau and Sears, 2014; Fisher and Anderson, 2015).

In the Sahel specifically, French-led operations failed to reverse the broader expansion of extremist violence or restore state legitimacy in countries such as Mali, Burkina Faso, and Niger (ICG, 2022). Civilian casualties, perceptions of external interference, corruption, and persistent underdevelopment contributed to declining local support for Western security interventions (UNDP, 2023). As RMVE organizations became increasingly decentralized and embedded within local conflicts and governance vacuums, conventional counterterrorism strategies struggled to adapt to the evolving nature of insurgency in many parts of Africa and especially in the Sahel region.

By 2024–2025, the Sahel recorded more than 11,000 annual fatalities linked to violent extremism, making it the deadliest terrorism theatre globally (Institute for Economics & Peace, 2025). This contemporary phase has been defined by the proliferation of organizations such as Jama'at Nusrat al-Islam wal-Muslimin (JNIM), Islamic State in the Greater Sahara (ISGS), and Islamic State West Africa Province (ISWAP), all of which operate through fluid and decentralized networks rather than fixed territorial strongholds (ICG, 2024). The evolution of terrorism in West Africa reflects a shift from fragmented and localized militancy to highly adaptive transnational insurgent networks embedded within regional political economies. Over time, weak governance and external interventions enabled extremist organizations to expand geographically and entrench themselves across the Sahel and the wider West African region.

Structural Drivers of Terrorism

The persistence and expansion of terrorism across Africa is rooted within a broader set of interconnected structural conditions that create permissive environments for instability, radicalization, and insurgent mobilization. Weak governance institutions, longstanding simmering conflicts and economies heavily

dependent on the exportation of primary commodities have combined to undermine state resilience and deepen societal vulnerabilities (Collier and Hoeffler, 2004; Fearon and Laitin, 2003). These structural weaknesses are further intensified by climate change, rapid urbanization, irregular migration flows, and persistent socioeconomic inequality, all of which contribute to competition over resources, displacement, and political marginalization (UNDP, 2023).

At the same time as discussed earlier, the growing nexus between organized crime and terrorism has transformed many extremist movements into hybrid political-criminal enterprises sustained through trafficking, smuggling, kidnapping, and illicit cross-border economies (UNODC, 2023). Advances in technology have further accelerated this transformation by enabling extremist organizations to expand propaganda, recruitment, financing, surveillance, and operational coordination across increasingly decentralized networks. Taken together, these structural drivers interact in mutually reinforcing ways, producing fragile environments in which violent extremist organizations are able not only to survive, but also to adapt, localize, and expand across national boundaries (Thurston, 2020; Walther and Christopoulos, 2015). The following section will examine how political, economic, environmental and technological pressures collectively shape the contemporary evolution of terrorism.

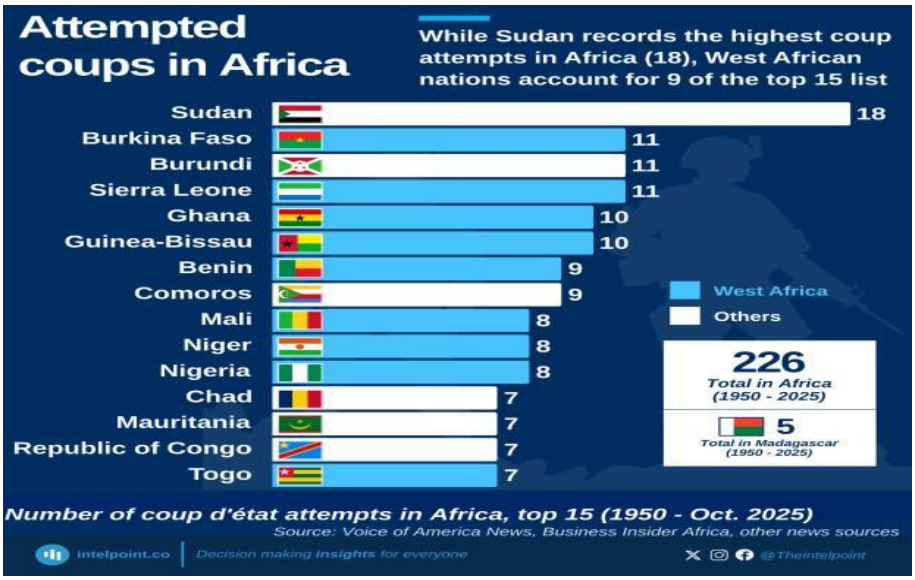
Structural Drivers: Politics

Many states in Africa and especially in West Africa are vulnerable to coup d'etat attempts this is due to weak institutions which often make it difficult to ensure stable transfers of power and effective civilian oversight of the military. Multiple factors including unemployment, and inequality can fuel public dissatisfaction with elected governments. In this challenging environment, military leaders have increasingly justified coups as necessary interventions to restore stability and security, even though such takeovers frequently deepen political instability rather than resolve it. Many states in West Africa are vulnerable to coups because their weak institutions often make it difficult to ensure stable transfers of power and effective civilian oversight of the military. Many states in this region are also impacted by the protracted insecurity due to the influence of extremist groups, this has helped weaken state authority and helped to increase the political influence of their armed forces.

The Soufan Center and ICG argue that regional instability has become self-reinforcing. Coups weaken democratic institutions, reduce foreign investment, and often damage relations with international partners, which can worsen economic decline and insecurity (The Soufan Center, 2023, ICG, 2024). At the same time, terrorist organizations and armed groups frequently exploit these periods of political uncertainty to expand their operations, especially where state authority is already fragile. Repeated coups in countries such as Mali, Burkina Faso, and Niger have

therefore not only reflected existing governance failures but have also contributed to a broader cycle of instability in which weak governance, insecurity, and military intervention continuously reinforce one another.

Attempted coups in Africa



Military Coups and New Security Alliances

Following successive military coups in Mali (2020–2021), Burkina Faso (2022), and Niger (2023), the Economic Community of West African States (ECOWAS) imposed sanctions, suspended the juntas from regional decision-making, and in the case of Niger, threatened military intervention to restore constitutional rule. The military juntas in Burkina Faso, Mali and Niger portrayed these measures as externally driven and punitive, arguing that ECOWAS had become overly aligned with French and Western interests rather than responding effectively to the region's escalating RMVE violence. This led to the withdrawal of Burkina Faso, Mali, and Niger from the Economic Community of West African States (ECOWAS) and the subsequent creation of the Alliance of Sahel States (Alliance des États du Sahel – AES). The AES reflected a convergence of security failures, political tensions, and growing anti-Western sentiment across the central Sahel. The formation of the AES in 2023–2024 represented both a collective security pact and a broader political rejection of the existing regional order (Reuters, 2024; AP News, 2025).

The deteriorating security environment in the Sahel was central to this rupture. Despite years of French, European, and American military assistance, insurgent violence linked to Jama'at Nasr al-Islam wal Muslimin (JNIM) and Daesh affiliates continued to expand across Mali, Burkina Faso, and Niger. Data from the Armed Conflict Location & Event Data Project (ACLED) indicates a sustained rise in militant attacks, territorial expansion by extremist groups, and increasing civilian fatalities

throughout the central Sahel (ACLED, 2025). Public frustration intensified as populations perceived both domestic governments and international partners as unable to restore stability or improve governance. The juntas increasingly framed sovereignty and self-reliance as essential to defeating terrorism, arguing that previous Western-backed counterterrorism frameworks had failed to restore territorial control or state legitimacy. The AES consequently emerged not only as a defense alliance but also as a symbolic project of political autonomy and resistance to what leaders characterized as “neo-colonial” influence (Reuters, 2024; IGC, 2024).

Russia played a significant role in facilitating this geopolitical realignment. According to the Center for a New American Security (CNAS), Moscow expanded its influence in the Sahel through security partnerships, Wagner Group deployments, military assistance, disinformation campaigns, and narratives emphasizing sovereignty and anti-colonial solidarity (CNAS, 2026). Russia positioned itself as an alternative partner unconstrained by Western governance conditions, appealing directly to military juntas focused on regime survival and security consolidation. In Mali especially, Wagner forces became embedded in counterinsurgency operations following the withdrawal of French troops, while Burkina Faso and Niger also deepened military and political engagement with Moscow. By contrast, China’s role has been more restrained and largely economic. Beijing has prioritized infrastructure investment, mining interests, and trade partnerships while avoiding direct military involvement in counterinsurgency campaigns. Nevertheless, both Russia and China have benefited strategically from the decline of Western influence and from growing Sahelian support for a more multipolar international order (CNAS, 2026; Soufan Center, 2024).

Persistent Conflict

Contemporary insecurity across Africa is increasingly shaped by the interaction of violent conflict, political instability, weak governance, and socioeconomic fragility. While the causes of conflict vary significantly across regions, many contemporary crises are rooted in these longstanding structural weaknesses. In several parts of the continent, these pressures have been further intensified by climate stress, rapid demographic change, and uneven development, contributing to growing instability and weakening the ability of states to maintain authority across peripheral regions (Fearon and Laitin, 2003; ICG, 2020). As a result, conflict environments have become increasingly fragmented and difficult to contain.

Across regions such as the Sahel, the Horn of Africa, Central Africa, and the Lake Chad Basin, violent conflict is now closely associated with declining public trust in state institutions, corruption, limited service delivery, and inadequate security. This has created permissive environments in which armed groups are able to consolidate

territorial influence, recruit marginalized populations, and exploit local grievances (Herbst, 2000; ISS, 2024). In countries such as the Democratic Republic of the Congo and Mozambique, insurgent and extremist organizations have embedded themselves within broader local conflicts, blurring the boundaries between terrorism, insurgency, criminality, and communal violence.

At the same time, recurring military coups and prolonged political instability have further undermined already fragile governance systems. In these contexts where state authority is largely absent, extremist movements are often able to operate with reduced risk of disruption while presenting themselves as alternative providers of security, justice, or economic opportunity. Consequently, terrorism in Africa is rarely driven by ideology alone. Rather, extremist violence frequently emerges from the interaction of unresolved political conflicts, economic marginalization all of which contribute to the erosion of state legitimacy and the persistence of cycles of violence (ACLED, 2024; ICG, 2020).

Weak Governance

The International Crisis Group (ICG) has highlighted how economic hardship and political exclusion contribute directly to state fragility. Many states continue to face high unemployment, food insecurity, and severe inequalities between urban centers and peripheral rural areas (ICG, 2023). In remote regions, particularly across the Sahel, governments frequently struggle to provide basic services such as security, education, healthcare, infrastructure, and economic opportunity. In these contexts, extremist organizations are often able to expand their influence by positioning themselves as the better alternative to the real political actors by offering not only alternative governance but also protection, dispute resolution, financial opportunities and even healthcare. (ICG, 2024, UNDP, 2023). Consequently, terrorism in many African contexts is closely linked not only to ideological radicalization, but also to broader failures of inclusion, governance and state-building.

Demographics

Demographic change represents both one of Africa’s greatest long-term opportunities and one of its most pressing structural challenges. The continent’s rapidly expanding and disproportionately youthful population has the potential to generate substantial economic growth and innovation. However, where demographic expansion is not matched by sufficient investment in education, and employment, it can also intensify social pressures and increase vulnerability to instability and extremist recruitment (United Nations DESA, 2022).

Africa is projected to experience the fastest population growth globally over the coming decades, with sub-Saharan Africa expected to expand by more than 70 per

cent by 2050 (Institute for Economics & Peace (IEP), 2024). Importantly, this growth is occurring most rapidly in states characterized by weak governance and constrained economic capacity. In many countries, governments are struggling to absorb growing demographic pressures. The *Ecological Threat Report* identifies demographic pressure as a major ecological and security stressor, particularly due to its role in accelerating urban expansion, increasing food demand, and intensifying pressure on already fragile infrastructure systems (IEP, 2021; 2024).

The relationship between population growth and resource scarcity is especially visible in food and water systems across sub-Saharan Africa. The region faces some of the world's most severe ecological pressures, driven by rising food insecurity, increasing water stress, environmental degradation, and rapid demographic expansion (IEP, 2024). As populations continue to grow, agricultural demand is expected to increase dramatically in several regions. Yet many agricultural systems remain highly vulnerable to climate change. Without major improvements in agricultural resilience, water management, and economic development, resource supply is unlikely to keep pace with demand. This imbalance risks exacerbating poverty, displacement, communal tensions, and political instability, all of which can create conditions conducive to conflict and extremist mobilization (IEP, 2024).

Structural Drivers: Economics

Demographic change is closely linked to broader structural features of African economies. Although the continent possesses vast reserves of natural resources and significant long-term economic potential, many states continue to face structural constraints that limit inclusive growth, economic diversification and institutional development. Dependence on the export of primary commodities, combined with demographic pressures has contributed to persistent economic vulnerability across several regions (UNCTAD, 2023; IMF, 2024).

Many African economies remain heavily reliant on the export of oil, minerals, and agricultural commodities as primary sources of national revenue. While these sectors generate substantial export earnings, they often produce relatively low levels of value-added economic activity compared to manufacturing and industrial production. Commodity-dependent economies are also highly exposed to fluctuations in global market prices, leaving many states vulnerable to external economic shocks, declining revenues, and fiscal instability (IMF, 2024). This dependence can weaken long-term development planning and reinforce patterns of economic inequality, particularly where revenues are poorly managed.

Demographic change further intensifies these structural pressures. Africa's rapidly expanding and youthful population represents a potentially transformative demographic dividend capable of supporting future economic growth and innovation.

However, in many states, job creation has failed to keep pace with labor market expansion, contributing to widespread youth unemploymentand low productivity growth (African Development Bank, 2024; United Nations, 2024). Although significant progress has been made in expanding access to education and healthcare, substantial gaps remain in skills development, technical education, and the creation of a productive workforce capable of competing in increasingly globalized economies (UNDP, 2023).

These economic challenges are compounded by inadequate transport systems, unreliable electricity supplies, weak digital connectivity, and limited industrial infrastructure. These factors significantly increase the cost of doing business. (World Bank, 2023). As a consequence, despite its large and rapidly growing population, Africa continues to account for a relatively small share of global GDP and global manufacturing output.

Weak state presence and limited security capacity across vast rural and border regions also constrain governments' ability to respond effectively to emerging threats. Consequently, terrorism and insecurity across Africa reflect a complex interaction of governance failures, economic exclusion, demographic pressure, and ecological stress rather than a single underlying cause (UNDP, 2017; ICG, 2020).

Persistent unemployment and widespread informal employment continue to heighten economic vulnerability across many African societies, especially among younger populations. Formal labor markets in many countries remain unable to absorb rapidly growing workforces, resulting in precarious livelihoods and limited economic mobility. Extremist organizations frequently exploit these conditions by offering financial incentives, social belonging, or integration into illicit economic systems involving smuggling, trafficking, taxation, and protection economies (ILO, 2023).

Groups such as Boko Haram in West Africa and al-Shabaab in East Africa initially emerged from local political and socioeconomic grievances, including poverty, marginalization, and distrust of government institutions. Over time, however, many of these groups strengthened their resilience by aligning themselves with transnational extremist movements such as DAESH and Al-Qaeda, thereby gaining access to additional resources, training, and ideological support (Botha, 2014; Thurston, 2017).

Nexus of Crime and Terrorism

Since 2024, drug trafficking routes connecting the Americas, Africa, and Europe have expanded substantially, with cocaine flows across the Atlantic increasing nearly sixfold. Simultaneously, Latin American criminal organizations, including the Cartel de Jalisco Nueva Generación (CJNG) and the Sinaloa Cartel, have sought to establish industrial-scale drug production in Africa by transferring technical expertise and using

the continent as both a production and transshipment hub. The discovery of methamphetamine laboratories operated with the involvement of Mexican cartel members in several African countries highlights the growing entrenchment of these networks. This nexus between organized crime and terrorism exacerbates existing governance and security vulnerabilities and enhances their operational and geographic reach. This worrisome development underscores the need for coordinated interagency and international responses.

Criminal actors are also profiting from the multiple conflicts impacting Africa. Especially the nexus between organized crime and terrorism in the Sahel has deepened considerably as a result of chronic state fragility, weak border governance, and long-standing informal trade networks. Across Mali, Niger, southern Algeria, and Libya, terrorist organizations have increasingly embedded themselves within existing smuggling economies that historically sustained nomadic and semi-nomadic communities, including many Tuareg groups whose livelihoods traditionally depended on trans-Saharan trade and mobility (Lacher, 2012).

The collapse of state authority following the 2011 Libyan civil war significantly accelerated this process. The fall of the Gaddafi regime released large quantities of weapons, fighters, and illicit trafficking routes into the Sahel, fueling insurgencies and strengthening armed non-state actors across Mali and neighboring states (UNODC, 2013). Terrorist organizations such as Al-Qaeda in the Islamic Maghreb (AQIM), Jama'at Nasr al-Islam wal Muslimin (JNIM), and Islamic State affiliates capitalized on these dynamics by integrating into trafficking networks involving arms, fuel, narcotics, migrants, and contraband goods.

Kidnapping for ransom (KFR) also became a major source of financing, with Western hostages generating millions of dollars for extremist groups during the 2000s and 2010s, thereby professionalizing militant networks and enabling territorial expansion (Botha, 2008; Lacher, 2012). This growing terrorist threat has also led to the growth of transnational criminal groups which are feeding off the conflicts creating an even greater crisis of internal displacement and migration. The aftermath of the Covid-19-pandemic and now the wars in Ukraine and in the Gulf will continue to create even greater economic downturns and feed burgeoning state fragility in the region.

The Global Peace Index 2026 identifies illicit resource extraction as an increasingly important driver of contemporary armed conflict, particularly in regions where state authority is weak and armed groups can capture economic assets (IEP, 2026). Competition over artisanal gold mining sites in Mali, Burkina Faso, and Niger has become a major driver of violence, with terrorist groups taxing gold production, controlling transport routes, and using gold as an alternative source of revenue outside formal banking systems (ICG, 2019). Gold smuggling networks now connect the Sahel

to markets in the Gulf, North Africa, and beyond, creating transnational financial ecosystems that sustain both organized crime and insurgency.

Across the Sahel, RMVE organizations including Jama'at Nasr al-Islam wal-Muslimin (JNIM) and Islamic State Sahel Province (ISSP) have expanded their presence around artisanal gold-mining sites in Mali, Burkina Faso, and Niger, where they generate revenue through informal taxation, protection rackets, extortion, and control of transportation corridors. Gold has become an especially valuable source of financing because it is portable, difficult to trace, and can be easily integrated into regional and global supply chains. The growth of artisanal mining across the Sahel has therefore provided armed groups with opportunities not only to enrich themselves but also to establish governance structures in remote areas where state institutions do not exist. In some cases, terrorist groups provide security to miners and traders in exchange for taxes and fees, thereby embedding themselves within local economies while simultaneously financing insurgent operations (IEP, 2026; ISS Africa, 2025). The strategic significance of these mining areas is reflected in the broader security environment, with terrorist groups increasingly expanding into regions containing major gold deposits and threatening mining infrastructure across West Africa (Reuters, 2026).

The Global Peace Index 2026 further demonstrates how conflict-related gold extraction has become integrated into wider transnational smuggling networks that connect African conflict zones to international markets (IEP, 2026). The report highlights Sudan as a particularly significant example, where gold has become a major source of conflict financing for armed actors. According to the Index, gold smuggling networks linked to the Sudanese conflict move substantial quantities of gold through neighboring states and onward to international markets, often beyond the reach of sanctions or regulatory oversight.

The report notes that imports of gold from countries with minimal domestic production, such as Chad and Libya, have increased dramatically, suggesting the existence of extensive cross-border smuggling routes. For example, United Arab Emirates customs data cited in the Global Peace Index show gold imports from Chad increasing from less than one ton in 2012 to approximately 18 tons in 2024, despite Chad possessing negligible domestic gold production. These discrepancies indicate the scale of illicit gold flows originating from conflict-affected regions and demonstrate how armed groups can exploit regional trading networks to monetize resource extraction (IEP, 2026). Such dynamics enable terrorist and insurgent organizations to reduce their dependence on external sponsors, increase their operational resilience, and sustain violence over prolonged periods. As a result, the convergence of terrorism, organized crime, and illicit gold extraction has become a defining feature of

contemporary conflict systems across parts of Africa, posing a complex challenge for both regional governments and international security actors.

The contemporary crime–terror financing ecosystem in Africa (2025–2026).

Terrorist organizations increasingly derive funding from a diversified portfolio of criminal activities, including illicit mining, drug trafficking, human smuggling and trafficking, arms trafficking, cyber-enabled crime, cryptocurrency-based finance, kidnapping-for-ransom, extortion, and informal taxation. These revenues are moved through both traditional and emerging financial mechanisms before being converted into operational capabilities that sustain insurgency, governance functions, recruitment, and territorial control. The chart illustrates the growing convergence of organized crime and terrorism across Africa, where illicit economies have become a

core component of terrorist funding which has greatly enhanced their resilience and sustainability.

Table II. Major Terrorist Groups in Africa, Principal Criminal Revenue Streams (2025–2026)

Terrorist Group	Primary Area of Operations	Key Criminal Activities	Strategic Effect
Jama'at Nasr al-Islam wal Muslimin	Mali, Burkina Faso, Niger	Kidnapping-for-ransom (KFR), livestock taxation, illicit gold mining, smuggling, extortion, protection rackets	Increasing reliance on taxation of local economic and artisanal mining
Islamic State Sahel Province	Niger, Mali, Burkina Faso	Extortion, illicit taxation, cattle rustling, arms trafficking, smuggling routes, gold mining	Strong control over rural transit corridors and local commerce.
Boko Haram	Northeastern Nigeria, Lake Chad Basin	KFR, cattle theft, taxation, human trafficking, fuel smuggling	Revenue diversified following territorial losses.
Islamic State West Africa Province	Nigeria, Niger, Chad, Cameroon	Taxation, fuel smuggling, fishing levies, agricultural taxation, extortion	One of Africa's most sophisticated terrorist financing systems.
Al-Shabaab	Somalia, Kenya	Taxation, charcoal trafficking, illicit trade, extortion, KFR, import/export levies	Generally assessed as the wealthiest terrorist organization in Africa.
Islamic State Somalia	Puntland, Somalia	Extortion, smuggling, crypto-enabled transfers, taxation	Increasing role as a regional financial hub for Islamic State networks
Allied Democratic Forces	Eastern DRC, Uganda	Gold trafficking, timber smuggling, taxation, human trafficking	Significant involvement in illicit mineral supply chains
Mozambique Islamic State Insurgency	Northern Mozambique	Ruby smuggling, heroin trafficking facilitation, timber trafficking, extortion	Benefits from proximity to major illicit maritime routes.

Structural Drivers: Environmental

Climate change has emerged as one of the most significant threat multipliers shaping insecurity, conflict, and human vulnerability across Africa. While environmental change is rarely a direct cause of terrorism or violent conflict, it increasingly intensifies existing political, economic, and social pressures, particularly in regions already characterized by weak governance and fragile livelihoods. Rising temperatures, changing rainfall patterns, droughts, floods, and desertification are placing growing strain on natural resources and contributing to heightened competition

over land, water, and agricultural production, especially across the Sahel and other ecologically vulnerable regions (IPCC, 2022).

The relationship between climate change and insecurity is particularly visible in agro-pastoral regions where livelihoods remain heavily dependent on rainfall-sensitive agriculture and livestock production. Environmental degradation and declining resource availability have increasingly fueled tensions between farming and pastoralist communities, creating local conflicts that extremist organizations are often able to exploit for recruitment, protection economies, or territorial influence. In this sense, climate change acts less as an isolated driver of violence and more as a force that amplifies pre-existing fragilities and governance failures (IEP, 2024).

The *Ecological Threat Report* identifies climate stress, food insecurity, and water scarcity as major ecological pressures likely to intensify instability across parts of Africa in the coming decades (IEP, 2021; 2024. Increasing temperatures are already reducing agricultural productivity and disrupting traditional livelihoods in regions such as the Sahel, where economic resilience and adaptive capacity remain limited. As ecological pressures converge with rapid population growth and weak governance, the risks of conflict, social unrest, and forced migration increase substantially.

These combined pressures are expected to contribute to large-scale internal displacement and cross-border migration throughout Africa over the coming decades. According to the *Ecological Threat Register*, more than one billion people already live in countries with low levels of resilience to ecological shocks, a figure expected to increase significantly as climate change accelerates (IEP, 2020). As livelihoods become increasingly unsustainable, migration from rural areas to urban centers, as well as international migration, is likely to intensify.

As climate change intensifies and demographic pressures grow, these groups are likely to expand geographically and operationally. In the Sahel's Liptako-Gourma region (bordering Mali, Burkina Faso, and Niger) and the Lake Chad Basin (Nigeria, Niger, Chad, and Cameroon), ecological stress combined with population growth is expected to deepen competition over land and water, fueling recruitment and conflict (IEP, 2024; UN, 2025). There is also increasing concern about the spread of these groups into coastal West African states such as Benin, Togo, and Ghana, where similar structural vulnerabilities are emerging (CFR, 2024). In this way, demographic and climate dynamics are not only shaping where terrorism persists, but also where it is most likely to expand by 2040.

High levels of human insecurity also create conditions in which extremist recruitment becomes more likely. Especially chronic poverty and food insecurity can deepen grievances against governments and weaken social cohesion. The interaction between climate changeand economic insecurity therefore has significant implications

not only for development and human security, but also for the future evolution of terrorism and political violence across Africa. The long-term implications of these dynamics extend beyond Africa itself. European policymakers, in particular, increasingly view instability, economic fragility, and demographic pressure across Africa as factors likely to intensify migration pressures in the coming decades, especially if economic development and political stability fail to keep pace with population growth (ISS, 2017).

Migration

The growing spread of terrorist movements across the Sahel and other parts of Africa has reinforced European concerns that instability in Africa could have direct consequences for European security through increased irregular migration, organized crime, and regional insecurity (EUISS, 2021). European Union and NATO member states increasingly view instability in Africa as a direct security challenge because of its connection to migration flows towards Europe. Migration has become a highly sensitive political issue within Europe because fears of uncontrolled migration flows has strengthened support for populist and extremist political parties across Europe. Since the 2015 refugee crisis, large migration movements have fueled anti-immigration rhetoric across many EU and NATO member states, contributing to political polarization and increasing pressure on democratic institutions (ISS, 2023). The political salience of migration has therefore evolved from a humanitarian concern into a central issue affecting electoral politics and democratic resilience across Europe.

European governments have responded by prioritizing migration control agreements with African states, often linking development aid and security cooperation to efforts aimed at reducing migration flows (ISS, 2023). Critics argue that this securitized approach risks undermining democratic values and human rights protections while simultaneously empowering authoritarian actors in partner countries (ISS, 2023). At the same time, European security institutions remain concerned that irregular migration routes could potentially be exploited by terrorist actors seeking access to Europe. While research indicates that there is limited empirical evidence directly linking migration and terrorism, policymakers continue to fear that weak border management, smuggling networks, and instability in transit regions may create opportunities for extremist infiltration (ISS Africa, 2025). The expansion of terrorist groups in the Sahel following the withdrawal of several Western military missions has intensified these concerns, particularly as violence and displacement continue to rise across West Africa (Reuters, 2024). Consequently, migration from Africa is increasingly framed not only as a humanitarian or economic challenge, but also as a strategic security issue with implications for European democracy, social cohesion and political stability.

As was shown, Africa's political, economic and environmental challenges are a deeply interconnected component of Africa's security and development landscape. At the same time Africa is also challenged by two other megatrends that are shaping the modern world, these include the rapid innovation and diffusion of new and emerging technologies and Africa's place in the current geopolitical and multipolar world context.

Megatrends: Technology

Africa is harnessing modern technology to leapfrog towards growth. At the same time, technology has substantially enhanced the capabilities, reach and adaptability of terrorist organizations. Terrorist groups have historically demonstrated a strong propensity to adopt new technologies when they are accessible, cost-effective and operationally advantageous. Drawing on the concept of 'lethal empowerment', it can be argued that violent non-state actors are often early adopters of technologies that increase their effectiveness and influence (Liang, 2023).

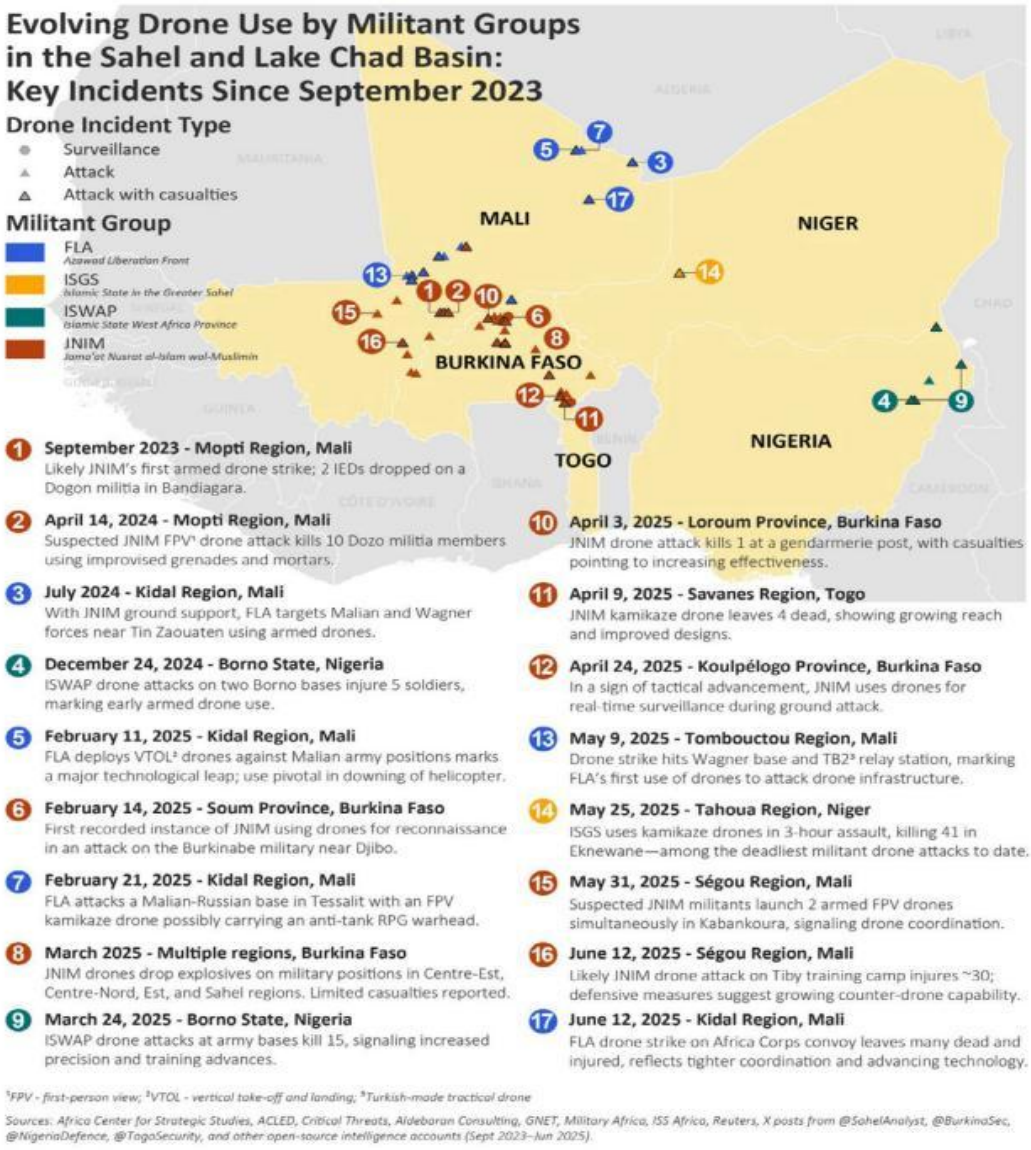
Technological developments have expanded the strategic and operational reach of terrorist organizations by enabling transnational communication, coordination and recruitment. Terrorist and violent extremist organizations in Africa are increasingly adopting digital communication technologies to enhance operational effectiveness, expand recruitment efforts and disseminate ideological narratives. Online platforms and social media have become powerful tools for radicalization.They provide extremists with unprecedented opportunities to influence vulnerable individuals, cultivate support networks and disseminate ideological narratives on a global scale (Liang, 2023).

Social media platforms, encrypted messaging applications and online forums provide opportunities to communicate securely across geographic boundaries, coordinate activities and maintain connections between dispersed networks. These technologies can also design recruitment campaigns with tailored local messaging. Terrorists are harnessing AI tools to translate their messages into multiple languages and dialects. These digital communication tools have strengthened the ability of terrorist organizations to influence audiences, mobilize supporters and sustain organizational resilience despite military and law-enforcement pressure.

In parallel, the adoption of commercially available drone technologies has provided new capabilities for intelligence, surveillance and reconnaissance (ISR). Drones can be used to monitor security force movements, gather battlefield intelligence, identify potential targets and improve situational awareness, allowing terrorist groups to enhance planning and operational decision-making while reducing risk to their personnel (Liang, 2024; ICG, 2022).

Alongside these developments, terrorist organizations are increasingly exploiting cyber-enabled activities and digital financial technologies to generate and move funds. Cybercrime, including online fraud, phishing schemes and identity theft provide terrorists with opportunities to acquire resources while operating across jurisdictions that are often difficult for authorities to police effectively. (INTERPOL, 2023; UNODC, 2022). At the same time, cryptocurrencies offer alternative mechanisms for fundraising, transferring funds and storing value outside traditional financial systems. The pseudonymous and transnational nature of many cryptocurrency platforms help complicate financial monitoring efforts and enable terrorist actors to receive donations, facilitate cross-border transactions and support operational activities with reduced visibility. (Financial Action Task Force (FATF), 2023; Liang, 2024). Together, the use of advanced communications technologies, drone-enabled ISR capabilities, cybercrime and cryptocurrency-based financing illustrates how terrorist organizations in Africa are adapting to the contemporary technological environment to achieve strategic, operational and financial advantages (Liang, 2023; FATF, 2023).

Beyond current online threats, emerging technologies such as uncrewed aerial systems (drones), artificial intelligence (AI), autonomous technologies and advanced cyber capabilities present new challenges for security practitioners and policymakers. Commercially available drones, for example, are relatively inexpensive, easy to operate and have already been employed by terrorist groups against military, diplomatic, infrastructure and civilian targets (Liang, 2024). These developments demonstrate how technological innovation continues to create new opportunities for terrorist actors, necessitating proactive and adaptive responses from governments, security agencies and civil society. The acquisition and use of drones by terrorist and insurgent groups has become a significant security challenge across Africa. Armed groups such as Boko Haram, the Islamic State West Africa Province (ISWAP), and al-Shabaab have increasingly employed commercially available unmanned aerial vehicles (UAVs) for intelligence gathering, surveillance, propaganda, and, in some cases, the delivery of explosive devices. The accessibility, relatively low cost, and ease of modification of civilian drones have enabled non-state actors to enhance their operational capabilities while reducing their exposure to conventional counterterrorism measures. This development has complicated military operations, increased the vulnerability of civilian populations, and expanded the geographical reach of terrorist attacks. Furthermore, weak border controls, limited regulatory frameworks, and the rapid growth of drone technology markets across Africa have facilitated the proliferation of UAVs among extremist groups. As a result, drone warfare is emerging as a critical security concern that requires enhanced regional cooperation, stronger regulatory oversight, and improved counter-drone technologies to mitigate the evolving threat posed by terrorist organizations (United Nations Office on Drugs and Crime, 2022; International Crisis Group, 2023).



The rapid spread of drones in Africa was initially driven by states seeking affordable alternatives to expensive conventional air forces. Many African governments, including those engaged in counterinsurgency operations, have acquired military UAVs such as the Turkish Bayraktar TB2, the Chinese Wing Loong II, and various surveillance drones to compensate for limited numbers of combat aircraft and constrained defense budgets. These systems have provided governments with enhanced intelligence, surveillance, reconnaissance, and precision-strike capabilities at a fraction of the cost of manned aircraft.

However, the growing availability of both military and commercial drone technology has also created opportunities for terrorist organizations to acquire similar capabilities. African governments have spent millions of dollars buying military grade drones, while terrorists groups have increasingly relied on cheap commercially available quadcopters, including modified DJI drones, for battlefield reconnaissance,

target acquisition, propaganda filming, and the delivery of improvised explosive devices. In February 2025, JNIM has taken drone attacks to the next level by executing its first recorded First-Person-View (FPV) drone attack on military positions in Djibo in Burkina Faso (Le Monde, 2025). Morocco's Policy Center for the New South reported that there were 30 drone attacks in the Sahel alone between September 2023 and June 2025, the majority of those 82% were conducted between March and June of 2025. One such attack by JNIM on a Malian military base in Boulikessi killed more than 100 soldiers.

Recent assessments indicate that militant terrorist groups in the Sahel continue to expand their operational reach and capabilities. A 2025 report to the United Nations Security Council identified Jama'at Nasr al-Islam wal Muslimin (JNIM) as capable of threatening regional capitals through its use of drone warfare and its freedom of movement across Burkina Faso, Mali and Niger (United Nations Security Council, 2025). The report further warned of JNIM's potential expansion into northern Togo, Benin and north-western Nigeria.

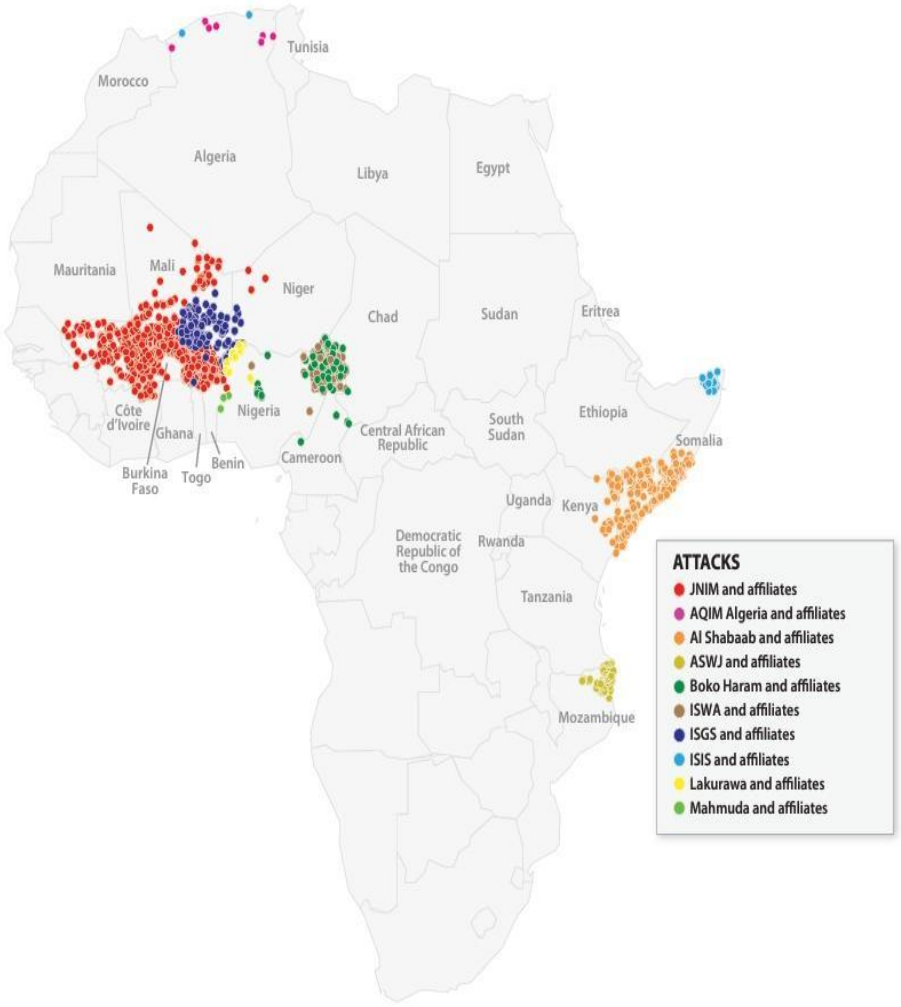
Similarly, Islamic State Sahel Province (ISSP) has increased both its territorial presence and recruitment efforts, establishing a significant base north of Niamey in Niger. In January 2026, ISSP demonstrated its growing capabilities through a coordinated attack on Niamey's international airport and Air Base 101 using drones and small arms (African Security Analysts, 2026). Analysts argue that the military coups in Burkina Faso, Mali and Niger between 2021 and 2023 weakened regional security cooperation, creating opportunities for both JNIM and ISSP to expand despite the establishment of the Alliance of Sahelian States (AES) (African Security Analysts, 2026).

The increasing movement of foreign fighters and the weakness of regional security structures have raised concerns that the Sahel may become a platform for wider transnational RMVE activity (South African Institute of International Affairs, 2026). Evidence of this trend includes Islamic State-linked networks facilitating attacks in Morocco and the growing connections between JNIM, ISSP and local militant groups in Nigeria.

Elsewhere in Africa, RMVE violence continues to evolve. In Somalia, fatalities increased significantly between 2024 and 2025 as both al-Shabaab and Islamic State-Somalia intensified operations. Islamic State-Somalia has emerged as an important financial and logistical hub for the wider Islamic State network, while al-Shabaab has reportedly strengthened its ties with the Houthi movement in Yemen. In Mozambique, violence linked to Ahl al-Sunnah wa al-Jama'a (ASWJ) increased by 51 per cent between 2024 and 2025 despite ongoing counterinsurgency efforts supported by Rwanda (Global Terrorism Index, 2026).

According to the 2026 Global Terrorism Index, militant organizations across Africa are increasingly adopting strategies aimed at economic disruption and coercion,

including blockades of major urban centers such as the one imposed by JNIM on Bamako in 2026 (Global Terrorism Index, 2026).



Note: Compiled by the Africa Center for Strategic Studies, this map shows violent events involving the listed groups for a year ending June 30. Group designations are intended for informational purposes only and should not be considered official. Due to the fluid nature of many groups, affiliations may change.
Sources: Armed Conflict Location & Event Data Project (ACLED); Centro Para Democracia e Direitos Humanos; Hiraal Institute; HumAngle; International Crisis Group; Institute for Security Studies; MENASTREAM; the Washington Institute; and the United Nations.

Looking ahead, drones are likely to play an even greater role in African conflicts as technology becomes cheaper, more autonomous, and more difficult to detect. The continued proliferation of UAVs could increase the frequency and sophistication of attacks by non-state actors, challenge state control over remote territories, and fuel regional instability unless effective counter-drone systems, export controls, and regulatory frameworks are implemented. Consequently, drones are expected to become a defining feature of both state and non-state warfare across Africa in the coming decade (Boulanin and Verbruggen, 2017; RUSI, 2024). They are reshaping African security and without proper management could have an important long term negative impact on the region. Extremist organizations have adapted by using commercial drones for reconnaissance, propaganda, and weaponization. Affordable drone technology has lowered barriers to asymmetric warfare, allowing non-state actors to challenge state forces more effectively (Boulanin and Verbruggen, 2017).

The procurement and growing indigenous market of drones in Africa is not the only technology that is having an important security impact in Africa, access to Starlink satellite internet access is also empowering violent extremist actors across Africa.

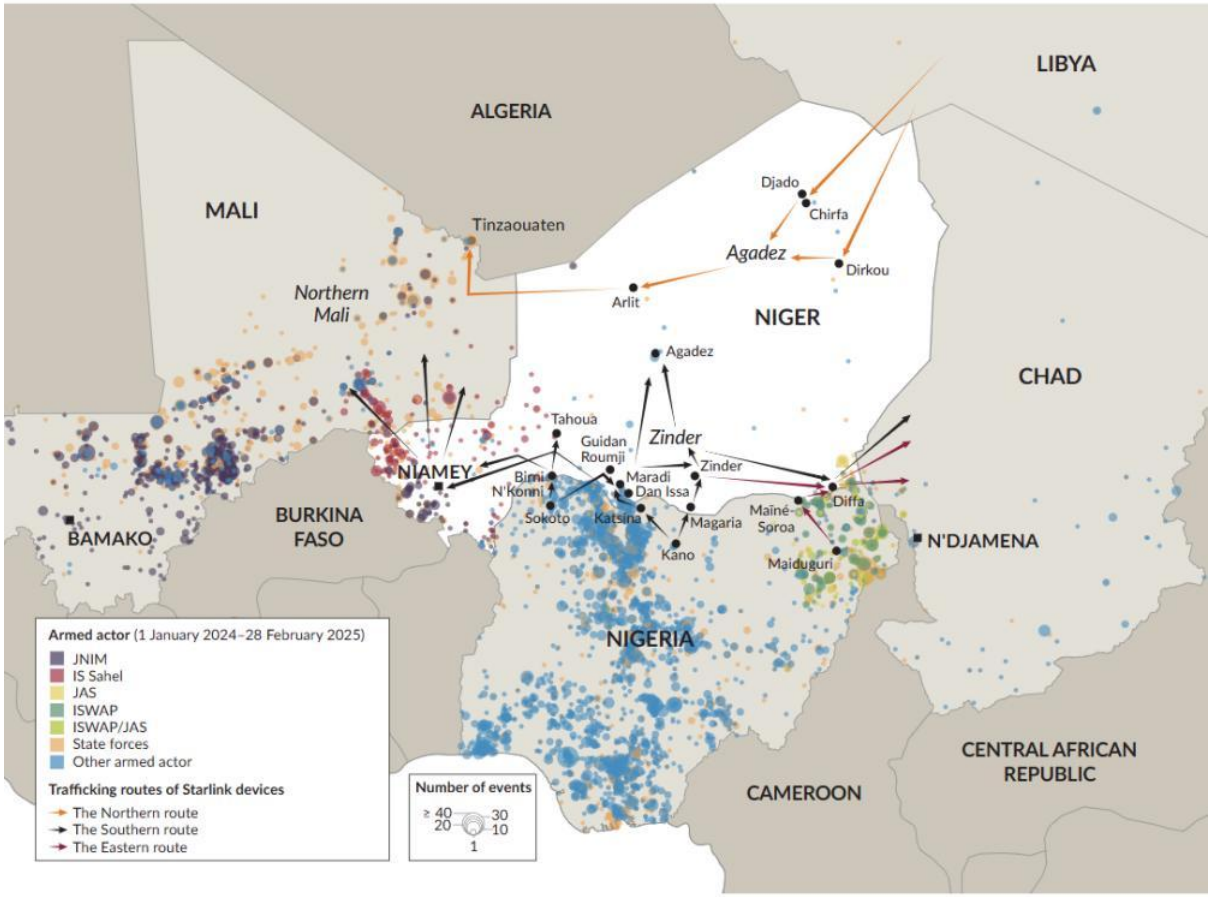
Especially the expansion of Starlink satellite internet across the Sahel has significantly altered the operational environment for both violent extremist organizations and criminal networks. Groups such as Jama'at Nasr al-Islam wal Muslimin (JNIM) and Islamic State West Africa Province (ISWAP) have increasingly exploited Starlink's portable satellite connectivity to strengthen secure communications, coordinate attacks in remote areas, and disseminate propaganda in regions with weak telecommunications infrastructure. Technology enables actors operating beyond state-controlled territory to evade surveillance and maintain operational resilience in environments where traditional mobile networks are unreliable or absent. As Sicolo argues, satellite internet technologies are becoming a critical enabler for extremist and criminal ecosystems due to their mobility, encryption potential, and independence from national infrastructure. (Sicolo, 2024) Security officials in Niger have similarly noted that the proliferation of Starlink devices has complicated intelligence interception efforts and enhanced the operational secrecy of armed groups operating across the central Sahel. (GIFCT, 2025) These developments occur within a broader regional security crisis, with the Sahel accounting for more than half of global terrorism-related deaths in 2024 (ReliefWeb, 2025).

At the same time, governments in the region are attempting to balance connectivity needs with security concerns. Niger and Chad legalized Starlink in 2025 in an effort to regulate the technology through device registration systems, while Mali has considered similar measures (Tanner, 2025; Höije, 2024). This type of legalization efforts reflects both developmental and security imperatives. Starlink offers substantially faster and cheaper internet access compared to existing state-owned providers, potentially reducing the digital divide in underserved rural areas. However, illicit supply chains continue to facilitate the circulation of unregistered devices among extremist groups and criminal actors seeking to avoid oversight. Consequently, while Starlink has the potential to improve digital inclusion and economic development, its rapid adoption also illustrates how emerging technologies can unintentionally intensify conflict dynamics, strengthen non-state armed actors, and complicate counterterrorism efforts in fragile regions.

The trafficking of Starlink kits across the Sahel illustrates how emerging technologies can rapidly become integrated into existing illicit economies and conflict infrastructures. Starlink kits are often dismantled into separate components, concealed among agricultural products, or transported via informal routes using motorbikes and unpaved roads to avoid detection (GIFCT, 2025). The illicit trade in Starlink kits has developed into a profitable transnational economy connected to extremist and criminal networks across the Sahel. Established smuggling corridors

linking Nigeria, Libya, Niger and northern Mali have become key routes for the movement of Starlink devices into areas controlled by armed groups, including territories influenced by JNIM and ISWAP. Major hubs such as Agadez, Maradi and Zinder serve as logistical nodes connecting urban supply chains to remote conflict zones in northern Mali and Niger. The trafficking and use of Starlink devices across the Sahel has become embedded within long-established smuggling corridors linking Nigeria, Niger, Chad, Libya, and northern Mali.

Starlink has substantially enhanced the operational capacities of criminal and extremist actors by enabling reliable, real-time communication across remote environments with limited telecommunications infrastructure. Traffickers themselves increasingly depend on the technology to coordinate logistics, evade law enforcement, and maintain communication networks across the desert.



Source: The shadow constellation: how Starlink devices are shaping conflict and crime in the the Sahel, Risk Bulletin #12, GIFCT, May 2025

The growing proliferation of Starlink across the Sahel demonstrates how digital innovation is reshaping both conflict dynamics and geopolitical influence in fragile regions. Policymakers face a difficult dilemma: while measures such as connectivity restrictions or geofencing could disrupt extremist communications, they may also undermine civilian access to connectivity and generate local resentment. Furthermore,

Starlink's geopolitical significance has increased because of the close relationship between the company and broader US strategic interests. As demonstrated in Ukraine, restrictions on Starlink access can have direct implications for military operations and conflict outcomes (Abels, 2024). Consequently, the growing dependence of armed actors on commercial satellite infrastructure may provide external powers with new forms of leverage over conflict dynamics in the Sahel, while also raising concerns about the privatization of strategic communications infrastructure in contemporary warfare.

Between 2020 and 2026, these dispersed militant networks evolved further into hybrid insurgent-criminal ecosystems embedded within transnational supply chains and weakly governed frontier regions. Rather than prioritizing continuous territorial occupation, groups such as JNIM, ISGS, and ISWAP increasingly focused on mobility, economic extraction, and indirect governance through taxation, control of smuggling routes, and manipulation of local grievances (UNODC, 2023). This evolution reflects a broader strategic adaptation in which insurgent organizations seek to control flows of goods, people, information, and resources across porous borders rather than conventional territorial administration. These groups rely heavily on cross-border mobility, local alliances, and criminal economies, enabling them to survive despite military pressure and territorial losses. The result is a highly adaptive conflict environment in which violence has become geographically expansive, and increasingly difficult to contain within national borders.

The contemporary phase of terrorism in West Africa is therefore defined not only by high levels of lethality, but also by the entrenchment of transnational militant systems that blur the boundaries between insurgency, organized crime, and local political economies (African Union, 2020; United Nations Development Programme, 2023). As a consequence, the Sahel has remained the global epicenter of terrorism, while violence has increasingly spread into coastal West African states, particularly along the Benin–Niger–Nigeria and Burkina Faso–Ghana–Côte d'Ivoire corridors where criminals and terrorists collaborate and collide.

Emerging Trends (2025–2026)

Several developments distinguish the current crime–terror nexus from earlier periods. First, illicit mining—particularly gold extraction in the Sahel and eastern DRC—has become one of the fastest-growing sources of terrorist financing, often rivaling kidnapping-for-ransom revenues. Second, migration-related crimes are becoming increasingly important, with terrorist groups taxing smuggling routes and providing protection services to trafficking networks moving migrants toward North Africa and the Mediterranean. Third, cyber-enabled finance is emerging as a new vulnerability. Although cryptocurrencies still represent a relatively small proportion of

overall terrorist financing in Africa, investigators have documented increasing use of cryptocurrency wallets, peer-to-peer exchanges, mobile banking, online fraud schemes, and digital financial facilitators to move funds across borders and evade sanctions or financial monitoring. (Soufan Center, 2024). Arms trafficking remains the critical enabling market that links terrorist and criminal ecosystems, sustaining insurgent expansion through flows of weapons originating from conflict zones in Libya, Sudan, the Sahel, and the Horn of Africa. In these fragile states where governance remains weak and security forces are under-resourced or politically contested, the convergence of illicit economies, technological adaptation, and extremist violence has created a resilient and highly adaptive conflict system that is increasingly difficult to dismantle through conventional military approaches alone (ACLED, 2025; Soufan Center, 2024).

The strategic significance of the crime–terror nexus lies not only in its contribution to terrorist financing, but in its role as a force multiplier that enables armed groups to embed themselves within local economies, diversify revenue streams, withstand military pressure, and maintain operational resilience across borders. Along with the diffusion of technology increasingly the widening geopolitical competition among the great powers is also fueling the growth of militant and terrorist groups.

Geopolitics

Geopolitical competition in Africa has become increasingly intertwined with the growth and persistence of terrorism, particularly across the Sahel, the Horn of Africa, and parts of Central Africa. External powers including France, the United States, the European Union (EU), NATO members, Russia, and China have all pursued strategic, economic, and security interests on the continent, often framing their engagement around counterterrorism, resource access, migration management, or geopolitical influence. However, critics argue that the overlapping agendas of these actors have at times weakened state legitimacy, intensified proxy rivalries, and contributed to conditions that militant organizations exploit. Terrorist groups such as Jama’at Nasr al-Islam wal Muslimin (JNIM), Islamic State Sahel Province (ISSP), Boko Haram, and al-Shabaab have repeatedly capitalized on public resentment toward foreign intervention, portraying governments as dependent on external powers and disconnected from local populations (Soufan Center, 2024; ACLED, 2025).

France has historically played one of the most influential external roles in West and Central Africa due to its colonial legacy and longstanding military presence. Operations such as Serval and Barkhane were launched to combat RMVE insurgencies in Mali and the wider Sahel, yet prolonged French military involvement gradually generated widespread anti-French sentiment. Many communities perceived France as prioritizing strategic influence, uranium access in Niger, and regional

political control rather than addressing governance failures and economic underdevelopment (Charbonneau, 2019).

The United States and the European Union similarly expanded their counterterrorism footprint after 9/11 through military training programs, intelligence partnerships, drone surveillance bases, and development aid linked to security cooperation. NATO's broader role has been indirect, primarily through capacity-building and partnerships with African states, particularly after the destabilizing effects of the 2011 Libya intervention.. Despite significant investment in security assistance, extremist violence has continued to spread, contributing to perceptions that external military approaches have failed to resolve underlying political and socioeconomic grievances.

Geopolitics and the Distribution of Modern Tech

In the new 'Scramble for Africa' geopolitics has played an important role in spreading modern technologies in Africa. Particularly the rapid spread of drones and digital surveillance systems, has become increasingly significant in terrorist capabilities and supporting counterterrorism strategies in Africa. The United States, France, Türkiye, China, Israel and Russia have all supplied or supported drone technologies across the continent. China has become a leading supplier of relatively inexpensive armed drones to African governments, and Russian military technologies have also expanded across the Sahel and Horn of Africa.

Russian cyber operations and disinformation campaigns also play a factor in the African the landscape. New foreign actors increasingly compete for influence through online propaganda, political manipulation, and information warfare. Consequently, technological competition in Africa is becoming inseparable from broader geopolitical struggles and the future trajectory of terrorism across the continent. These megatrends are but some of the multiple factors that are driving insecurity in Africa. Another important aspect is that in trying to fight extremism in Africa, African countries have made some difficult security choices that have not always led to more peaceful results especially as regards collaborating with private military companies.

Russia's Return to Africa

Russia has emerged as a major geopolitical actor in Africa by presenting itself as an alternative to Western powers. Through Wagner Group deployments, military agreements, arms sales, and disinformation campaigns, Moscow has expanded influence in countries such as Mali, the Central African Republic, Libya, and Sudan

(CNAS, 2026). Russia's approach has appealed particularly to authoritarian governments and military juntas seeking regime security without Western conditions related to democracy or human rights.

In return, Russia has gained access to mining concessions, strategic resources, and political influence. According to General Anderson, Africa has become "Putin's Purse," since 2022 gold extractions alone across the Sahel and Central African Republic have generated over $2.5 billion which has allowed Russia to sustain its economy which has been under strain due to the sanctions imposed on it for its illegal invasion of Ukraine in 2022. This allows Russia to insulate and protect its regime while limiting NATO's reach on its southern flank. According to the Africa Center for Strategic Studies, Russia is also actively recruiting thousands of vulnerable youths to fight for it on the frontlines of Ukraine. With the help of shadowy network of online recruiters, Russia is funneling thousands of Africans from nearly every country on the continent into the front lines and factories supporting Moscow's war effort in Ukraine. Many are lured with promises of jobs and training abroad, only to end up fighting in Ukraine (Africa Center for Strategic Studies, 2026). At the same time, Russia is also feeding an active disinformation campaign designed to obstruct further engagement of NATO, AFRICOM and the EU. Russia is attempting to insulate Africa from the West - at the same time it is extracting its resources and exploiting its people. Wagner-linked operations have also been associated with allegations of human rights abuses and civilian violence, which can further fuel radicalization and recruitment by extremist groups (The Soufan Center, 2024).

China's Expanding Impact in Africa

China's engagement differs significantly in that it has focused primarily on economic influence through infrastructure investment, mining, telecommunications, energy projects, and the Belt and Road Initiative. China has become Africa's largest bilateral trading partner, motivated by access to critical minerals, rare earth resources, oil, strategic shipping routes, and expanding consumer markets (Alden and Large, 2019). While Beijing generally avoids direct military intervention, its economic footprint contributes to geopolitical competition and concerns regarding debt dependency, digital surveillance technologies, and strategic influence over African governments. China's security cooperation also includes extensive military training programs, joint exercises and arms sales. China's security engagement in Africa cannot be separated from the Belt and Road Initiative (BRI) which has expanded China's strategic and economic footprint across Africa through investments, in energy infrastructure, ports, railways, roads and industrial zones. Given China's economic exposure and investment it has a lot to offer Africa while at the same it wants to protect its investments.

Nantulya argues that the ultimate objective of the BRI is to create a new global system of economic, political and security interdependencies centered on China (Nantulya, 2024). The establishment of China's first overseas military base in Djibouti symbolizes this transformation whose many roles include anti-piracy operations, peacekeeping logistics and protection of Chinese nationals. Through the Forum on China-Africa Cooperation (FOCAC), China has expanded its military and security engagement with Africa while at the same time China is one of the top ten contributors of personnel to UN peacekeeping missions (Lammich, n.d.). China's strategy is to present itself as a responsible global power while simultaneously expanding it geopolitical reach by institutionalizing its long-term commitments to supporting the African Standby Force and the African Capacity for Immediate Response to Crises (ACIRC) (Lammich, n.d.).

The competition among these external powers contributes indirectly to terrorism by reinforcing fragile governance structures and intensifying local grievances. Many African states remain heavily dependent on foreign military assistance, resource extraction contracts, or geopolitical patronage networks that often benefit political elites more than local populations. Extremist groups exploit narratives of corruption, foreign exploitation, and state weakness to recruit supporters and justify insurgency. In regions where governments are viewed as externally controlled or unable to provide security and services, terrorist organizations can present themselves as alternative authorities. Moreover, the growing militarization of counterterrorism responses has at times displaced civilian governance initiatives and deepened cycles of violence. According to ACLED data, areas experiencing heavy military operations frequently continue to experience high levels of civilian casualties and retaliatory extremist attacks (ACLED, 2025). The spread of new technologies, especially drones and Starlink internet access has further accelerated the technological prowess of extremist groups. Geopolitical competition is increasing instability especially when security priorities do not include governance reform, development and economic inclusion. As has been shown political insecurity, economic insecurity, governance challenges, technological challenges and geopolitics are important factors that are impacting Africa's broader security and development landscape. Given all the structural problems and mega trends happening in Africa what should NATO's role be in helping Africa to counter all these burgeoning threats and challenges.

NATO's Role in Africa

In order to prepare for the evolution of terrorism in Africa until 2040, it is important to not only use strategic anticipation to assess how these challenges will evolve in the future but also to analyze how resilient Africa is to these complex security challenges. Are African states sufficiently strong enough, resilient enough and

adaptive enough to respond to these contemporary and emergent threats? Are Africa's government institutions and security institutions sufficiently fit for the job ahead? What steps, if any, should NATO take to deliver greater stability, security, peace and prosperity to the region while at the same time ensuring that its own security is assured in its own backyard?

Future engagement may therefore focus on indirect support through AU and African-led frameworks, including intelligence-sharing, logistics, border security assistance, counter-extremism financing, and institutional capacity-building rather than large-scale troop deployments. Such an approach seeks to contain the spread of instability into coastal West African states while avoiding the political backlash associated with earlier Western military interventions. However, persistent governance failures, military rule, economic fragility, and intensifying geopolitical competition suggest that the long-term trajectory of the AES remains highly uncertain.

Africa's Strategic Relevance: NATO's Southern Neighborhood

Africa has become increasingly important to NATO because instability on the continent is now seen as directly connected to European and transatlantic security interests (Šikl, 2021). Rather than being viewed as geographically distant, regions such as North Africa, the Sahel, and the Horn of Africa are increasingly considered part of NATO's wider "southern neighborhood," where insecurity can spill over into Europe through terrorism, migration pressures, organized crime, and regional conflicts. As a result, instability in Africa is now being reassessed. Concerns that the Sahel could evolve into a broader zone of chronic instability or extremist sanctuary have intensified debate regarding on whether NATO and external actors should support African Union (AU)-led stabilization efforts. While direct NATO intervention remains politically sensitive given strong anti-Western sentiment across the AES (Alliance des *États du Sahel*) analysts from CNAS, the Soufan Center, and ACLED argue that a complete Western withdrawal risks strengthening the extremist groups and expanding Russian influence in West Africa (Soufan Center, 2024; ACLED, 2025).

NATO's increasing focus on the southern neighborhood reflects a recognition that instability across the Middle East, North Africa, and the Eastern Mediterranean has direct implications for Euro-Atlantic security (NATO, 2025). According to NATO Secretary General's Special Representative for the Southern Neighborhood, Javier Colomina, Türkiye has also played an influential role in shaping NATO's Southern Neighborhood Action Plan, which seeks to strengthen cooperation with regional and international organizations such as the African Union (AU), European Union (EU), United Nations (UN), Gulf Cooperation Council (GCC), and Arab League (Anadolu Agency, 2026). Türkiye has emerged as a central component of NATO's evolving

“360-degree” security strategy, particularly regarding the alliance’s southern flank and Mediterranean security architecture.

NATO officials have emphasized Türkiye’s strategic geographic position, military capabilities, and expanding defense industry as critical assets in maintaining regional deterrence and stability. Türkiye also plays an essential role in securing Mediterranean maritime routes and countering terrorism. NATO’s southern engagement strategy increasingly emphasizes political dialogue, defense cooperation, capacity-building, and partnership frameworks rather than direct military intervention. Within this structure, Türkiye functions as both a frontline NATO member affected by regional instability and a diplomatic bridge between the alliance and actors across the Mediterranean, Middle East, and parts of Africa. Türkiye participates actively in NATO partnership frameworks such as the Mediterranean Dialogue and the Istanbul Cooperation Initiative. These initiatives reflect NATO’s broader attempt to manage interconnected regional threats while reinforcing collective security and strategic coordination (Demir and Tarhan, 2026).

The United States, as the leading power within NATO, is also positioned to play a significant role in reshaping Western engagement with Africa, particularly as several African states continue to express interest in stronger strategic partnerships. The US Africa Command (AFRICOM) unlike NATO has legal and logistical mechanisms to operate in Niger, Mali and Somalia. The relationship between AFRICOM and NATO is comprehensive. Many AFRICOM officers are former NATO veterans and NATO’s operability standards underpin much of the United States training provided to African militaries. At the same time many of the exercises like African Lion, Flintlock and Obangame Express are jointly staffed by NATO countries and NATO’s Association of African Air Forces (AAAF) is backed by both the United States and NATO allies. However, NATO needs to define its relationship with AFRICOM more clearly and could benefit from greater coordination to ensure that their relationship is less competitive and more complementary.

Recommendations for NATO engagement in Counterterrorism Cooperation in Africa

NATO’s current role in Africa is best described as supportive, rather than strategic or operational. NATO lacks a formal mandate and is more reactive than proactive focusing on threats emanating from Africa rather than Africa itself. Africa should no longer be viewed as being on the periphery of transatlantic security thinking and Africa needs greater support from its allies and friends. In order to secure a better future for Africa, NATO’s engagement in Africa will likely revolve around four main strategic priority pillars: good governance and security cooperation; intelligence and

information sharing; training and capacity building; and operational and logistical support.

Good Governance and Security Cooperation

NATO should support good governance and support diplomatic normalization and regional security cooperation by developing stronger partnerships were urgently needed. NATO should thus encourage and support efforts to restore constructive diplomatic engagement between ECOWAS member states and the AES (Alliance of Sahel States) as a foundation for more effective regional counterterrorism cooperation across West Africa and the Sahel. Persistent political divisions have weakened collective security mechanisms and limited the ability of states to respond to increasingly transnational terrorist threats.

In the medium term all 32 NATO allies should adopt an “Africa-focused Southern Flank Framework” under the existing Southern Neighborhood Action Plan. The Framework should define Africa as the priority sub-region of the southern flank, with an initial focus on North Africa, West Africa, the Sahel and regional maritime routes. This framework would include four deliverables: a common threat assessment on non-state actors in Africa; a coordination mechanism for an Allied national initiative, a partner-driven capacity-building option for African states and regional organizations and short-, medium- and long-term planning on NATO’s core objectives.

This would give NATO a clearer political mandate. In order to strengthen the analytic capability, the framework should task the Strategic Direction South Hub, in coordination with NATO’s Joint Intelligence and Security Division (JIS), with producing a shared Southern Corridor threat assessment linking developments across Libya, the central Sahel, and Mediterranean maritime routes. Integrating intelligence on Russian security partnerships, trans-Saharan trafficking corridors, and armed-group mobility into a common Allied baseline would allow NATO to align national initiatives more effectively while reinforcing its role as a coordination framework.

Particular attention should be given to Russian security partnerships and influence activities across Africa, including military cooperation agreements, private military networks, disinformation campaigns, and arms transfers, which have expanded in several African states in recent years (International Crisis Group, 2024; SIPRI, 2025). The assessment should also integrate intelligence on trans-Saharan trafficking corridors, illicit financial flows, and the mobility of armed groups operating across porous borders in the Sahel and North Africa. Establishing a common Allied baseline for these threats would enable NATO members to align national initiatives more effectively, enhance strategic foresight, and reinforce NATO’s role as a coordination framework rather than a direct security provider (NATO, 2022).

NATO should establish an annual coordination forum on Africa, chaired by the Special Representative for the Southern neighborhood and supported by the Hub. This forum could map allied activities, identify gaps and develop common principles of engagement. Its agenda should include Russian, China, counterterrorism, maritime routes, defense education and partner request. Over time, this could become NATO's main mechanism for aligning Allied efforts in Africa without creating a new permanent mission. This would strengthen cohesion by showing Southern Allies that their threat perceptions are institutionally recognized.

NATO should develop a maritime cooperation package that coordinates Operation Sea Guardian with partner capacity-building efforts in North Africa and selected West African coastal states. This package should focus on enhancing maritime domain awareness, port security, information sharing, search and rescue coordination, and counter-trafficking training. NATO should frame this cooperation around shared security interests: protecting vital trade routes, disrupting criminal networks, strengthening coastal resilience, and preventing extremist groups and hostile state actors from exploiting maritime vulnerabilities. Such an approach would provide NATO with a practical, non-escalatory role that directly contributes to Allied security while supporting regional stability.

Strengthening cooperation along this maritime corridor would also improve NATO's ability to monitor risks affecting critical energy infrastructure, submarine communications cables, and commercial shipping routes connecting the Gulf of Guinea, the Mediterranean, and the wider Indo-Pacific region. The strategic importance of these maritime networks is underscored by the vulnerability of key chokepoints such as the Bab-el-Mandeb Strait and the Suez Canal. Together, these waterways constitute one of the world's most important maritime corridors, facilitating a substantial share of global trade and energy flows between Europe, Asia, and the Middle East (UNCTAD, 2024). Recent assessments highlighted in the Global Peace Index 2026 demonstrate how insecurity in the Red Sea region and disruptions to shipping transiting the Bab-el-Mandeb Strait can have cascading effects on international supply chains, increase transportation costs, and generate wider economic and security consequences for Europe and the broader international community (Institute for Economics & Peace, 2026).

Better integration between Operation Sea Guardian's situational-awareness outputs and partner-capacity initiatives in North and West Africa would enable the Alliance to anticipate how coastal instability, maritime crime, and disruptions along the Bab-el-Mandeb–Suez corridor may translate into wider southern-flank security risks (Institute for Economics & Peace, 2026). By enhancing maritime resilience across Africa's Atlantic and Red Sea littorals, NATO would contribute not only to regional

stability but also to the protection of critical global trade routes upon which Allied economic and security interests depend (UNCTAD, 2024).

Intelligence and Information Sharing

NATO should prioritize support for practical confidence-building measures that strengthen operational cooperation across borders. These measures may include the development of shared border-security frameworks, support for joint standard operating procedures (SOPs), enhanced intelligence-sharing arrangements, mutual legal assistance mechanisms, and coordinated approaches to incident response. Existing bilateral and trilateral security initiatives can serve as entry points for rebuilding trust and interoperability.

NATO should expand support for counter-terrorist financing and logistics disruption. NATO should place greater emphasis on assisting regional partners in disrupting the financial and logistical networks that sustain terrorist organizations. While military operations remain important, long-term degradation of terrorist capabilities depends equally on denying access to revenue streams, supply chains, and facilitation networks. Support efforts should focus on strengthening regional capabilities to identify and disrupt illicit economic activities associated with terrorism financing, including exploitation of artisanal mining areas, livestock markets, fuel distribution networks, informal transportation systems, and cross-border trading corridors. NATO can contribute through capacity building, technical assistance, and support for intelligence-led investigations that target the economic foundations of terrorist activity.

Training and Capacity Building

As regards training and capacity building it is important that NATO prioritizes counter-unmanned aerial systems (C-UAS) capabilities as a core component of its security assistance to African partner states. NATO should prioritize counter-unmanned aerial systems (C-UAS) capabilities as a core component of its security assistance to African partner states. The rapid proliferation of commercially available unmanned aerial systems (UAS) has fundamentally altered the operational environment in many African conflict zones, enabling both state and non-state actors to conduct reconnaissance, intelligence gathering, target acquisition, propaganda dissemination, and, increasingly, precision attacks at relatively low cost (Institute for Economics & Peace, 2026; NATO, 2024). The Global Peace Index 2026 argues that technological diffusion is lowering the barriers to entry for non-state armed groups, enabling them to project power more effectively (Institute for Economics & Peace, 2026). Consequently, counter-drone measures should be viewed not as a niche capability but as a critical requirement for maintaining operational effectiveness and force protection in contemporary security environments.

NATO assistance should therefore focus on providing field-proven detection, tracking, identification, and mitigation systems capable of operating in austere and infrastructure-poor environments. Capacity-building initiatives should prioritize scalable and sustainable technologies that can be integrated into existing command-and-control structures while remaining affordable for partner states with limited defense budgets (NATO, 2024). Support could include portable radio-frequency detection systems, ground-based radar systems optimized for small drones, electro-optical sensors, electronic-warfare capabilities, and operator training programs.

Equally important is the development of doctrinal and institutional capacities, including threat assessment procedures, intelligence fusion mechanisms, and operational concepts for countering drone-enabled threats. Integrating these capabilities into border-security forces, rapid-reaction units, and critical infrastructure protection frameworks would improve situational awareness, provide early warning of hostile activity, and strengthen the resilience of partner states against both terrorist organizations and other destabilizing actors operating across Africa's increasingly contested security landscape (Institute for Economics & Peace, 2026; NATO, 2024).

At the regional level, NATO should support the development of common counter-UAS standards, operational procedures, and training curricula. Incorporating counter-drone scenarios into multinational exercises and partner training activities would strengthen interoperability and improve preparedness for emerging threats.

Operational and Logistical Support

NATO should encourage partner governments to establish structured public–private security partnerships that leverage the rapidly expanding ecosystem of commercial intelligence and analytics providers. Commercial OSINT, GEOINT, satellite imagery, and advanced analytical platforms increasingly provide timely and scalable insights that complement traditional intelligence capabilities.

Rather than relying solely on transactional procurement models, NATO should promote frameworks that integrate commercial analytical capabilities into national and regional security decision-making processes. This includes supporting the use of commercial GEOINT and satellite-derived products for threat assessments, border monitoring, and operational planning.

NATO should also encourage the development of legal and regulatory frameworks that facilitate responsible information sharing between governments and private-sector partners. Such frameworks should balance security requirements with protections for data sovereignty, privacy, and commercial interests. Particular attention should be given to AI-enabled analytical tools that enhance intelligence

fusion, digital forensics, identity resolution, and pattern-of-life analysis while maintaining appropriate human oversight and evidentiary standards.

NATO should develop a counter-disinformation support offer for African partners, focused on resilience rather than propaganda. This could include training for strategic communications officials, support for crisis management, media literacy partnerships, open source monitoring, and exchanges with NATO STRATCOM experts. The program should be offered through partner requests and where possible, coordinated with the EU and African civil society organizations. NATO must be careful not to appear as if it is managing African information spaces. The objective should be to help partners identify manipulation, protect public institutions, and communicate transparently during crises. This would directly constrain Russian influence while avoiding the avoiding the reputational risks of over information warfare.

NATO should also encourage greater regional cooperation through structured financial intelligence exchanges and joint investigations targeting interconnected crime-terror networks operating across the Sahel and Coastal West Africa. NATO could help support strengthening Financial Intelligence Units (FIUs), enhancing financial investigative capabilities, improving asset-tracing and asset-freezing mechanisms, and supporting the harmonization of legal frameworks related to terrorist financing as well as increasing greater collaboration with the work being conducted by INTERPOL.

Over the longer term, NATO should support the gradual re-establishment of a cooperative regional security architecture capable of facilitating coordinated planning, operational interoperability, and collective responses to evolving threats across West Africa and the Sahel. NATO should support the institutionalization of intelligence fusion as a central pillar of regional counterterrorism cooperation. Effective fusion mechanisms improve situational awareness, accelerate threat detection, and facilitate coordinated responses to transnational terrorist activity.

Rather than creating new institutions, NATO should focus on strengthening existing national and regional structures by improving interoperability, analytical standards, and information-sharing arrangements. Support should include reviews of mandates, memoranda of understanding (MoUs), and technical systems to ensure that national fusion centers are effectively connected to regional coordination frameworks.

NATO can also provide assistance in developing secure communications infrastructure, common analytical methodologies, and mechanisms for joint threat assessments and coordinated preventive operations. While political reconciliation processes may progress unevenly across the region, practical intelligence cooperation

and operational coordination should be pursued wherever conditions permit in order to address immediate security challenges.

NATO Strategic Priorities - Good Governance and Security Cooperation			
Strategic Priorities	**NATO Objective**	**Priority Actions**	**Strategic Effect**
diplomatic normalization and regional cooperation	rebuild regional security cooperation and interoperability	support confidence-building measures, border-security frameworks, intelligence-sharing arrangements, and regional dialogue	improved coordination against transnational terrorist threats
adopt a short “Africa-focused Southern Flank Framework” under the existing Southern Neighborhood Action Plan.	provide a coherent strategic framework for NATO's engagement in Africa.	establish a dedicated Africa-focused framework that aligns NATO's counterterrorism, resilience, maritime security, and partnership activities with clearly defined regional priorities and objective	improves strategic coherence, reduces fragmentation, and strengthens NATO's ability to address security challenges emanating from Africa.
establish an annual coordination forum on Africa, chaired by the Special Representative for the Southern neighborhood and supported by the Hub	improve coordination and information sharing across NATO and partner stakeholders.	convene an annual forum led by the Special Representative for the Southern Neighborhood to review threats, coordinate activities, and align priorities among Allies, partners,	strengthens situational awareness, policy coherence, and collective responsiveness to emerging security challenges in Africa

		and relevant organizations.	
Training and Capacity Building			
Strategic Priorities	**NATO Objective**	**Priority Actions**	**Strategic Effect**
NATO should develop a maritime cooperation package coordinating Operation Sea Guardian with partner capacity-building	strengthen maritime security and counterterrorism cooperation across the Mediterranean and adjacent African maritime regions.	integrate operation Sea Guardian activities with targeted maritime capacity-building, intelligence sharing, and joint training for African partner navies and coast guards	enhances partner maritime security capabilities, disrupts terrorist and illicit networks, and improves interoperability and stability across key maritime corridors
counter-terrorist financing and logistics disruption	degrade terrorist operational capacity	strengthen FIUs, support financial investigations, target illicit economic networks, and promote legal harmonization	reduced terrorist access to revenue, logistics, and facilitators
counter-drone capability development	Enhance force protection and civilian security	Provide counter-UAS training, technologies, doctrine development, and interoperability support	Increased resilience against evolving aerial threats
Operational and Logistics Support			
Strategic Priorities	**NATO Objective**	**Priority Actions**	**Strategic Effect**
Public–Private security partnerships	expand access to actionable intelligence and technology	integrate commercial GEOINT, OSINT, satellite imagery, and AI-enabled	faster decision-making and improved situational awareness

		analytics into security workflows	
sustainable unclassified intelligence sharing	improve information exchange across partners	develop common reporting standards, verification processes, and sustainable intelligence practices	enhanced regional coordination and early warning
regional intelligence fusion	strengthen collective threat detection and response	support fusion centers, secure communications, joint assessments, and interoperability frameworks	more effective disruption of transnational terrorist networks
support the gradual re-establishment of a cooperative regional security architecture to evolving threats across West Africa and the Sahel	capable of facilitating coordination and planning	support operations, interoperability and collective responses	more effective disruption of transnational terrorist networks at the regional level

Table 1. Strategic Priorities for NATO Engagement in Africa

Conclusion

As was presented, terrorism in Africa is not driven by a single factor but is being reinforced by multiple megatrends -- conflict and war, demographics, climate change, geopolitics, and today's modern technological revolution.. Together, these megatrends create a potent combination of interconnected factors that increasingly empower violent non-state actors. These factors have dramatically impacted human security, the conduct of modern warfare, and the dynamics of geopolitical competition. As a result, terrorism in Africa is not only a security issue but has become a much broader geopolitical challenge that will continue to be an important security threat in 2040.

NATO still maintains a relatively limited footprint in Africa, however its engagement with the continent has gradually expanded through partnerships with the

African Union (AU), capacity-building initiatives, and security operations in the Mediterranean, including Operation Sea Guardian. These activities reflect NATO's recognition of the interconnected nature of Euro-Atlantic and African security, particularly in addressing transnational threats such as terrorism, piracy, and irregular migration. However, NATO's growing role must be understood within the broader normative framework of African ownership and strategic autonomy.

The phrase "African solutions to African problems," coined by the Ghanaian economist George Ayittey in response to the Somali crisis of the 1990s, has since become a foundational principle of the African Union's peace, security, and governance agenda. The concept reflects the belief that African states and regional organizations are best positioned to understand and address the continent's political, economic, and security challenges through locally driven institutions and mechanisms (African Union, 2013). It is particularly evident in regional security initiatives led by the African Union (AU), the Economic Community of West African States (ECOWAS), the EAS and the Intergovernmental Authority on Development (IGAD). Such efforts seek to strengthen African ownership, reduce long-term dependence on external actors, and enhance the legitimacy and sustainability of conflict resolution across the continent (Williams, 2017). Consequently, while NATO can play an important supporting role through partnership, training, intelligence sharing, and logistical assistance, its involvement is generally viewed as most effective when it complements, rather than directs, African-led initiatives. This balance aligns with the broader aspirations for sovereignty, regional integration, and sustainable development articulated in the AU's Agenda 2063 framework (African Union Commission, 2015).

At the same time given that Africa has become the world’s epicenter of terrorism in the last two years and that a new ‘terrorist domino effect’ is occurring where terrorist groups are continuously expanding their recruitment base and reach show that the Africans and their neighbors must work together. The complexity of this now global challenge demonstrates that no continent can operate in isolation from wider international dynamics. Furthermore, the international system is increasingly characterized by geopolitical competition among major global powers, with Africa becoming a key arena for strategic influence. The growing involvement of powers such as the United States, Russia, China, Türkiye, the European Union, the Gulf states and NATO reflects a renewed competition over resources, trade routes, security partnerships, technology, and diplomatic influence. While African states benefit from diversified partnerships and investment opportunities, this geopolitical “scramble” also risks deepening external dependency and strategic fragmentation. Consequently, although African-led approaches remain essential, durable peace and development require constructive cooperation with global institutions and international partners.

Ultimately, “African Solutions for African Problems” should not be interpreted as isolationism but rather as a framework for empowered partnership and shared responsibility. The interconnected nature of today’s world means that Africa’s future is inseparable from global political and economic developments. In an era defined by global megatrends and strategic competition among major powers, African agency must therefore be complemented by inclusive multilateralism and genuine international partnership.

NATO can play an important complementary role in supporting African security and long-term sustainability through partnerships that prioritize capacity building, institutional strengthening, and cooperative security rather than external domination. While NATO does not maintain a permanent military presence in Africa, it has become increasingly strategically relevant in ensuring that security challenges can be mitigated and that Africa’s future will be more prosperous and more resilient.

NATO’s partnerships with the African Union, ECOWAS, AFRICOM, EU, UN and other regional organizations can contribute to enhancing peace support operations, maritime security, disaster response, and defense expertise. In addition, NATO can contribute indirectly to sustainability by supporting stability conditions necessary for economic development, humanitarian access, and climate adaptation initiatives. Such cooperation would be most effective if framed within genuine multilateral partnerships that recognize African agency and avoid perceptions of geopolitical competition or neo-colonial influence. Most importantly, NATO’s future engagement should focus on supporting democratic governance, civilian oversight of armed forces, rule of law, and resilience against the abuse of new technologies, disinformation and violent non state actors, while fully respecting African ownership and sovereignty. International support should prioritize countries demonstrating a commitment to good governance by investing in stabilization efforts and reinforcing local institutions dedicated to peace and security. Together, these mutually reinforcing strategies provide a comprehensive framework for NATO to help enhance Africa's stability, resilience, and long-term prosperity.

References

Acemoglu, D. and Robinson, J. (2012) *Why Nations Fail: The Origins of Power, Prosperity, and Poverty*. New York: Crown.

ACLED (2024) *Armed Conflict Location & Event Data Project: Africa Overview*. Providence, RI: ACLED.

ACLED (2024) *Armed Conflict Location & Event Data Project: Global Analysis Trends*. Providence, RI: ACLED.

ACLED (2024) *Armed Conflict Location & Event Data: Sahel Conflict Trends Report*. Washington DC: ACLED.

ACLED (2025) *Africa: Non-state Armed Groups are the Main Drivers of Violence Targeting Local Officials*. Available at: ACLED.

ACLED (2025) *Conflict trends and political violence in Africa*. Armed Conflict Location & Event Data Project.

ACLED (2025) *Conflict trends in the Central Sahel*. Armed Conflict Location & Event Data Project.

ACLED (2025) *What's Driving Conflict Today? A Review of Global Trends*. Available at: ACLED (Accessed: 14 May 2026).

ACLED (2024) *Armed Conflict Location & Event Data Project: Conflict Trends Report 2024*. Providence: ACLED.

Africa Center for Strategic Studies (2024) *Enhancing Counterterrorism Coordination in Coastal West Africa: Read Ahead Paper*. Washington DC: ACSS.

Africa Center for Strategic Studies (2026) *Russia's deceptive war recruitment scheme ensnares thousands of young Africans*. 19 May.

African Centre for the Study and Research on Terrorism (2023) *Terrorism Situation and Trend in Africa*. Algiers: African Union.

African Development Bank (2024) *African Economic Outlook 2024*. Abidjan: African Development Bank.

African Development Bank (2024) *African Economic Outlook 2024*. Abidjan: African Development Bank.

African Union (2013) *50th Anniversary Solemn Declaration*. Addis Ababa: African Union.

African Union Commission (2015) *Agenda 2063: The Africa We Want*. Addis Ababa: African Union Commission.

African Union Commission (2025) *African Union calls for urgent action in insurgency hit Mali*. Reuters, 10 November.

African Union (2020) *AU Master Roadmap of Practical Steps to Silence the Guns in Africa*. Addis Ababa: African Union Commission.

Alden, C. and Large, D. (2019) *New Directions in Africa–China Studies*. London: Routledge.

Amnesty International (2024) *Mali: Accountability Concerns in Security Operations*. London: Amnesty International.

Anadolu Agency (2026) ‘Türkiye key to NATO deterrence, southern stability, alliance official says’, *Anadolu Agency*, 18 February.

AP News (2025) *What’s ahead for a 50-year-old West African bloc after 3 junta-led countries left the group?* Associated Press.

Botha, A. (2008) *Terrorism in the Maghreb: The Transnationalisation of Domestic Terrorism*. Pretoria: Institute for Security Studies.

Botha, A. (2014) *Radicalisation in Kenya: Recruitment to al-Shabaab and the Mombasa Republican Council*. Pretoria: Institute for Security Studies.

Boulanin, V. and Verbruggen, M. (2017) *Mapping the Development of Autonomy in Weapon Systems*. Stockholm: SIPRI.

Center for a New American Security (CNAS) (2026) *Beyond the Sahel: Russia’s Toolbox for Influence in Africa*. Washington, DC: CNAS.

Charbonneau, B. (2019) ‘Intervention in Mali: Building Peace Between Peacekeeping and Counterterrorism’, *Journal of Contemporary African Studies*, 37(4), pp. 415–431.

Charbonneau, B. and Sears, J. (2014) *Choc Therapy: Diagnosing the Mali Crisis*. Ottawa: Centre for International Policy Studies.

Council on Foreign Relations (2024) *Violent Extremism in the Sahel*.

Council on Foreign Relations (2026) *Global Conflict Tracker Update: Sub-Saharan Africa Terrorism Trends*.

Council on Foreign Relations (2026) *Violent Extremism in the Sahel*. New York: CFR Global Conflict Tracker.

Chris Devonshire-Ellis, C. (2020) ‘84% of China’s BRI Investments Are in Medium-High Risk Countries’, *Silk Road Briefing*, 2 July.

Coffey, D. (2021) ‘Senegal Calls on China to Intervene in Sahel Anti-Jihadist Operations’, *Radio France Internationale*, 29 November.

Demir, G.N. and Tarhan, M. (2026) ‘Türkiye key to NATO deterrence, southern stability, alliance official says’, *Anadolu Agency*, 18 February.

Dizolele, M.P. (2025) ‘NATO expansion into Africa faces structural limits amid great power competition’, *Center for Strategic and International Studies (CSIS)*.

Downs, E., Becker, J. and de Gategno, P. (2023) *China’s Ports in Africa*. Washington DC: Brookings Institution.

EUISS (2017) *Out of (and inside) Africa: Migration Routes and Their Impacts*. Paris: European Union Institute for Security Studies.

EUISS (2020) *Sahel Climate Conflicts? When (Fighting) Climate Change Fuels Terrorism*. Paris: European Union Institute for Security Studies.

EUISS (2021) *Salafi-Jihadism in Africa*. Paris: European Union Institute for Security Studies.

Europol (2024) *Terrorism Situation and Trend Report (TE-SAT) 2024*. The Hague: Europol.

Fearon, J.D. and Laitin, D.D. (2003) 'Ethnicity, insurgency, and civil war', *American Political Science Review*, 97(1), pp. 75–90.

Fisher, J. and Anderson, D.M. (2015) 'Authoritarianism and the securitization of development in Africa', *International Affairs*, 91(1), pp. 131–151.

Herbst, J. (2000) *States and Power in Africa: Comparative Lessons in Authority and Control*. Princeton: Princeton University Press.

Höije, K. (2024) 'Mali lifts ban on Musk's SpaceX in bid to control Starlink usage', *BNN Bloomberg*, 10 October.

Institute for Security Studies (ISS) (2024) *Conflict Trends in Africa 2024*. Pretoria: Institute for Security Studies.

International Crisis Group (2020) *Violence and Governance in the Sahel*. Brussels: International Crisis Group.

ILO (2023) *World Employment and Social Outlook: Trends 2023*. Geneva: International Labour Organization.

IMF (2024) *Regional Economic Outlook: Sub-Saharan Africa*. Washington DC: International Monetary Fund.

Institute for Economics & Peace (2020) *Ecological Threat Register 2020*. Sydney: Institute for Economics & Peace.

Institute for Economics & Peace (2021) *Ecological Threat Report 2021*. Sydney: Institute for Economics & Peace.

Institute for Economics & Peace (2024) *Ecological Threat Report 2024*. Sydney: Institute for Economics & Peace.

Institute for Security Studies (ISS) (2017) *African Futures and Migration Dynamics*. Pretoria: Institute for Security Studies.

International Crisis Group (2020) *Violence and Governance in the Sahel*. Brussels: International Crisis Group.

Interview with security official in Niamey (2025) March.

IPCC (2022) *Climate Change 2022: Impacts, Adaptation and Vulnerability*. Geneva: Intergovernmental Panel on Climate Change.

Iderawumi, M. (2022) 'Why Small Satellite Constellations are the Next Revolution for Africa', *Space in Africa*, 30 May.

IGC (2024) *Political Transitions and Regional Fragmentation in the Sahel*. International Growth Centre.

Institute for Economics and Peace (2020) *Ecological Threat Register*. Sydney: Institute for Economics and Peace.

Institute for Economics and Peace (2021) *Ecological Threat Register 2021*. Sydney: Institute for Economics and Peace.

Institute for Economics and Peace (2024) *Ecological Threat Report 2024*. Sydney: Institute for Economics and Peace.

Institute for Economics and Peace (2024) *Global Terrorism Index 2024*. Sydney: Institute for Economics and Peace.

Institute for Security Studies (ISS) (2024) *African Conflict and Security Analysis*. Pretoria: ISS Africa.

International Crisis Group (2019) *Getting a Grip on Central Sahel's Gold Rush*. Brussels: International Crisis Group.

International Crisis Group (2020) *Conflict Dynamics in Africa*. Brussels: International Crisis Group.

International Crisis Group (2020) *Violence in the Sahel: Trends and Responses*. Brussels: International Crisis Group.

International Crisis Group (2023) *The Challenges of Governance and Security in the Sahel*. Brussels: International Crisis Group.

International Crisis Group (2024) *Coups and Political Instability in West Africa*. Brussels: International Crisis Group.

International Crisis Group (2024) *The Sahel: Fragile States and Armed Group Dynamics*. Brussels: International Crisis Group.

International Crisis Group (2024) *The Sahel: Tackling the Rise of Extremism*. Brussels: International Crisis Group.

International Labour Organization (ILO) (2023) *Global Employment Trends for Youth 2023*. Geneva: ILO.

International Crisis Group (2021) *Cameroon's Far North: A New Front in the Fight Against Boko Haram*. Brussels: International Crisis Group.

International Crisis Group (2023) *The Risks of Intensifying Conflict in Coastal West Africa*. Brussels: International Crisis Group.

International Crisis Group (2024) *Digital Dimensions of Jihadist Insurgency in the Sahel*. Brussels: International Crisis Group.

International Crisis Group (2024) *Sahel and Coastal West Africa: Fragmentation and Security Cooperation Challenges*. Brussels: International Crisis Group.

International Crisis Group (2024) *The Risks of Fragmented Security Responses in the Sahel*. Brussels: International Crisis Group.

International Crisis Group (2024) *The Sahel Crisis and Expanding Regional Insecurity*. Brussels: International Crisis Group.

International Crisis Group (2022) *After Mali, Barkhane and the Future of Counterterrorism in the Sahel*. Brussels: International Crisis Group.

International Monetary Fund (IMF) (2024) *Regional Economic Outlook: Sub-Saharan Africa*. Washington DC: IMF.

International Monetary Fund (IMF) (2024) *World Economic Outlook 2024*. Washington DC: IMF.

INTERPOL (n.d.) *Partnerships against terrorism*.

INTERPOL (2018) *Transnational crime converging across Africa*. 14 December.

IPCC (2022) *Climate Change 2022: Impacts, Adaptation and Vulnerability*. Geneva: Intergovernmental Panel on Climate Change.

ISS Africa (2023) *Africa-Europe Migration Deals Cost Lives and Undercut Democracy*. Pretoria: Institute for Security Studies.

ISS Africa (2025) *Lessons from Africa on Terrorism*. Pretoria: Institute for Security Studies.

Jaura, R. (2025) ‘NATO in Africa: Why the Transatlantic Alliance Is Turning South – Analysis’, *Eurasia Review*, 15 July.

Jeune Afrique (2025) ‘Alliance des États du Sahel : où en est vraiment l’intégration ?’, 5 July.

Lacher, W. (2012) *Organized Crime and Conflict in the Sahel-Sahara Region*. Washington DC: Carnegie Endowment for International Peace.

Liang, C.S. (2017) *The Leaderless Jihad in a Leaderless World: The Future of Terrorism*. Geneva: Geneva Centre for Security Policy.

Liang, C.S. (2023) *Technology and Terror: From Dynamite to the Metaverse*. Geneva: Geneva Centre for Security Policy.

Liang, C.S. (2024) *Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies*. Geneva: Geneva Centre for Security Policy.

Mamoudou, O. (2025) 'Starlink désormais disponible au Niger', *Studio Kalangou*, 14 March.

Moe, L.W. and Simojoki, M.V. (2023) 'Great power competition in Africa: implications for peace and security', *Conflict, Security & Development*, 23(2), pp. 115–132.

Moumouni, A.K. (2024) 'Révolution numérique : le Niger signe un partenariat avec Starlink pour offrir un Internet fiable à tous', *ActuNiger*, 30 October.

Nantulya, P. (2024) *China's Expanding Security Role in Africa*. Washington DC: Africa Center for Strategic Studies.

National Space Research and Development Agency (2023) *Nigeria's Space Capabilities and Security Applications*. Abuja: NASRDA.

NATO (2023) *Cooperation with the African Union*.

NATO (2024) *NATO and the African Union*. Brussels: North Atlantic Treaty Organization.

NATO (2025) *Deterrence and Defence*.

NATO (2022) *Open Source Intelligence Handbook*. Brussels: NATO Cooperative Cyber Defence Centre of Excellence.

Notte, H. (2025) 'Russia Is Shrewdly Playing the Long Game in Africa', *War on the Rocks*, 17 September.

Nsaibia, H. and Weiss, C. (2020) 'The Growing Complexity of Violent Extremism in the Sahel', *CTC Sentinel*, 13(11), pp. 1–15.

OECD (2022) *States of Fragility 2022*. Paris: Organisation for Economic Co-operation and Development.

Organisation for Economic Co-operation and Development (2022) *Cross-Border Dynamics and Security Challenges in the Sahel*. Paris: OECD Publishing.

Organisation for Economic Co-operation and Development (2022) *Cross-Border Security and Governance in West Africa*. Paris: OECD Publishing.

Organisation for Economic Co-operation and Development (2023) *Border Security and Illicit Economies in the Sahel and Coastal West Africa*. Paris: OECD Publishing.

People’s Republic of China (2015) *Counterterrorism Law of the People’s Republic of China*. Beijing: State Council of the People’s Republic of China.

People’s Republic of China (2021) *The 14th Five-Year Plan for National Economic and Social Development of the People’s Republic of China*. Beijing: State Council Information Office.

ReliefWeb (2025) *Global Terrorism Index 2025*.

Reuters (2024) *Junta-led Sahel states rule out return to West African economic bloc*. 6 July.

Reuters (2024) *West Africa becomes global terrorism hotspot as Western forces leave*.

Reuters (2026) *Mali attacks show expanding reach of Sahel militant groups*. Available at:

Reuters (2026) *Mali conflict situation report and leadership updates*. Available at:

Rodney, W. (2018) *How Europe Underdeveloped Africa*. London: Verso.

Russia Matters (2025) ‘Russia Analytical Report, Sept. 15–22, 2025’, *Russia Matters*.

Sicolo, G. (2024) ‘Dark signals: the growing threat of satellite internet in extremist networks’, *Global Network on Extremism and Technology*, 18 December.

Tanner, J. (2025) ‘Starlink launches in Niger, signs operator licence in Chad’, *Developing Telecoms*, 17 March.

Thurston, A. (2017) *Boko Haram: The History of an African Jihadist Movement*. Princeton: Princeton University Press.

Šikl, V. (2021) *NATO in Africa*. Prague: Prague Student Summit Background Report. Available at: Prague Student Summit Background Report.

Soufan Center (2024) *Security and Geopolitical Competition in the Sahel*. New York: The Soufan Center.

The Soufan Center (2023) *The Crisis in the Sahel: Coups, Extremism, and Fragile States*. New York: The Soufan Center.

The Soufan Center (2024) *Militant Groups and Security Dynamics in the Sahel*. New York: The Soufan Center.

The Soufan Center (2024) *Security Governance and State Fragility in Africa*. New York: The Soufan Center.

The Soufan Center (2025) *JNIM Expanding Geographic Reach and Staging Coordinated Attacks in the Sahel*.

The Soufan Center (2025) *Sub-Saharan Africa Remains an Epicenter of Violent Jihadist Terrorism*.

The Soufan Center (2026) *Al-Qaeda Affiliate in the Sahel Could Topple the Government in Mali*. *IntelBrief*, 27 April.

Shinn, D.H. (2025) 'Russia Plays the Long Game in Africa', *The Official Blog of Amb. David H. Shinn*, 17 September.

Thurston, A. (2020) *Jihadists of North Africa and the Sahel: Local Politics and Rebel Groups*. Cambridge: Cambridge University Press.

Toulemonde, M. (2025) 'Sahel : comment les jihadistes cherchent à encercler les villes de l'AES', *Jeune Afrique*, 31 May.

Transparency International (2023) *Corruption Perceptions Index 2023*. Berlin: Transparency International.

UNCTAD (2023) *Economic Development in Africa Report 2023*. Geneva: UNCTAD.

UNCTAD (2023) *Economic Development in Africa Report 2023*. Geneva: United Nations Conference on Trade and Development.

UNDP (1994) *Human Development Report 1994*. New York: United Nations Development Programme.

UNDP (2023) *Journey to Extremism in Africa: Pathways to Recruitment and Disengagement*. New York: United Nations Development Programme.

UNDP (2023) *Journey to Extremism in Africa: Pathways to Recruitment and Disengagement*. New York: United Nations Development Programme.

United Nations (2024) *World Economic Situation and Prospects 2024*. New York: United Nations.

UN DESA (2022) *World Social Report 2022: Leaving No One Behind in an Ageing World*. New York: United Nations.

UNDP (1994) *Human Development Report 1994: New Dimensions of Human Security*. New York: UNDP.

UNODC (2013) *Transnational Organized Crime in West Africa: A Threat Assessment*. Vienna: United Nations Office on Drugs and Crime.

UNODC & UNICRI (2023) *UNODC and UNICRI Launch a New Project to Address the Nexus Between Terrorism and Organized Crime in Africa*.

UNODC & UNICRI (2024) *Assessing and Addressing the Nexus Between Organized Crime and Terrorism in Africa*.

United Nations (n.d.) *Reports and Briefings on Security and Humanitarian Conditions in the Sahel Region*. UNOWAS / Security Council.

United Nations (2023) *Report of the Secretary-General on the Situation in the Sahel*. New York: United Nations.

United Nations (2023) *World Social Report 2023: Leaving No One Behind in an Ageing World*. New York: United Nations.

United Nations (2024) *World Population Prospects 2024*. New York: United Nations.

United Nations (2025) *Secretary-General's Remarks on Counter-Terrorism in West Africa and the Sahel*. New York: United Nations.

United Nations Development Programme (2023) *Human Development Report 2023/24*. New York: UNDP.

United Nations Development Programme (2023) *Journey to Extremism in Africa: Pathways to Recruitment and Disengagement*. New York: UNDP.

United Nations Development Programme (2024) *Human Development Report 2024*. New York: UNDP.

United Nations Office on Drugs and Crime (2023) *Transnational Organized Crime and Terrorism in the Sahel*. Vienna: UNODC.

United Nations Office on Drugs and Crime (2023) *Transnational Organized Crime and Terrorism in West Africa: Border Security Challenges*. Vienna: UNODC.

United Nations Office on Drugs and Crime (2023) *Transnational Organized Crime and Terrorism in West Africa: Border Security Dynamics*. Vienna: UNODC.

United Nations Office on Drugs and Crime (2023) *Transnational Organized Crime and Terrorism in West Africa: Border Security and Institutional Challenges*. Vienna: UNODC.

United Nations Office on Drugs and Crime (2024) *Terrorism, Technology and Organized Crime in the Sahel*. Vienna: UNODC.

Warner, J. and Charles, M. (2026) 'Assessing African Jihadist State Takeovers: Capability, Will, and the Puzzling Logic of Inaction', *Hudson Institute*.

Weimann, G. (2016) *Terrorism in Cyberspace: The Next Generation*. New York: Columbia University Press.

Williams, P.D. (2017) *Fighting for Peace in Somalia: A History and Analysis of the African Union Mission (AMISOM), 2007–2017*. Oxford: Oxford University Press.

World Bank (2023) *Africa's Pulse: An Analysis of Issues Shaping Africa's Economic Future*. Washington DC: World Bank.

World Bank (2023) *World Development Report 2023*. Washington DC: World Bank.

World Bank (2024) *World Development Indicators*. Washington DC: World Bank.

Xi, J. (2021) *Speech on the Belt and Road Initiative and Maritime Development*. Beijing: Government of the People's Republic of China.

Zenn, J. (2023) *Digital Jihadism and Militant Propaganda in Africa*. Washington DC: Jamestown Foundation.

CHAPTER 5

Future of Terror-Crime Nexus

Dr. Vanda Felbab-Brown and Diana Paz Garcia

Abstract

Over the next two decades, emerging technologies will weaken the crime-terrorism nexus by reducing incentives for cooperation between organized crime and terrorist organizations. Historically, this nexus has been sustained by shared dependence on territorial control, labor-intensive operations, logistical cooperation, and mutual protection. However, advances in technology are enabling criminal and terrorist groups to operate more independently and with greater functional self-sufficiency. Moreover, for each type of violent actor, new technologies are reducing dependence on territory for revenue generation and complex logistical chains. New technologies are enabling financing without territorial control, violent operations with much reduced labor and cross large distances, and in-house supply production of contraband and weapons. AI-enabled finance and cybercrime are de-territorializing illicit revenue generation, while additive manufacturing and drones reduce reliance on transnational supply chains. At the same time, automation is diminishing the need for manpower. Paradoxically, although these innovations increase operational efficiency, they also undermine one of the traditional sources of resilience for illicit groups: their ability to build local legitimacy by serving as employers in marginalized communities. Some terrorist groups will seek to control territories and run independent "states" as their sine qua non purpose. But for many, as well as for criminal groups, data, digital infrastructure, and cybersecurity will be replacing territory and labor as the primary strategic assets and the focus of contestation with governments. While certain territories, such as those hosting data centers, critical minerals, water resources, or strategic maritime access, will retain or even gain strategic importance, state sponsorship is likely to become more valuable than crime-terror cooperation because states can provide advanced technological capabilities, intelligence, and safe havens that nonstate actors cannot. The chapter concludes by outlining policy priorities, including strengthening data security, regulating additive manufacturing, and mitigating AI-driven unemployment, which could expand the appear of violent nonstate armed actors.

Introduction

Political violence and economic crime have long been intertwined in what scholars have termed the crime–terror nexus. The relations between terrorist and

other militant organizations, pro-government militias, criminal groups, and illicit economies have long been fluid, adaptive, and multidimensional. They evolve in response to shifting incentives, environmental pressures, and changes in the global security landscape. Actors on the ideology-profit motive intersect through various forms of cooperation and convergence, sharing financial, logistical, human, and technological resources and learning from each other. But they also engage in fierce, including violent competition, with each other (Felbab-Brown, 2019).

Over the next two decades, this nexus will undergo a profound transformation. Technological innovation, digital globalization, and accelerating environmental change are reshaping the strategic environments in which illicit actors operate. Artificial intelligence (AI), cryptocurrencies, unmanned and autonomous systems, remote communication tools, and decentralized online marketplaces are expanding the means of coordination and financing beyond traditional territorial constraints. But they are also dramatically reducing some of the reasons why politically-motivated violent actors reached out to criminal groups and formed cooperative relationships with them. The two actors will also become far less dependent on each other.

These intertwined processes are driving a restructuring of both criminality and politically-motivated violence and the nexus between the two: criminality and politically-motivated violence will require far less labor for the production of illicit goods, such as drugs, services, and violence itself. Remote platforms will allow both crime and any kind of violence to be conducted over great distances by a few people.

Terrorists, militants, and criminals will also become far less dependent on physical territories for accomplishing and facilitating many of their objectives– including the ability to conduct attacks, raise money for their operations, and procure weapons.

The far smaller requirements for labor and physical territories will, in turn, mean that both criminal and militant groups will lose a lot of political capital they obtained from serving as employers, such as from their sponsorship of labor-intensive illicit economies like drug cultivation and from maintaining large standing armies (Felbab-Brown, 2010).

Only some territories will matter, such as those hosting large data centers and containing resources for their operations, like water, rare earth and metals, and energy production, and those that can act as physical safe havens from the reach of governments or rivals. For both groups, the most precious assets to acquire will be a) the ability to breach data of their rivals – states, private actors, general populations, and other nonstate armed groups - and b) secure their own data from hostile breaches.

Why Criminals and Terrorists Used to Get Together

Since the end of the Cold War, scholars have analyzed why and how terrorist, militant, and criminal organizations intersect and interact, and, indeed, transform as a result of interacting with each other. They have emphasized that the exact nature of their relationship varies across a wide spectrum. Proposing a typology of interactions, Phil Williams emphasized that the crime-terror relationship is dynamic and context-dependent rather than falling into rigid categories (Williams 2012). On one side of the spectrum, what he called the convergence model, he described varied cooperative exchanges between the two types of actors, such as swapping arms for drugs or sharing smuggling routes, between otherwise distinct actors. On the other side of the spectrum, what he labeled as a transformative model, militant groups abandoned their political motivations and became principally driven by economic objectives, essentially evolving into criminal groups.

Tamara Makarenko highlighted that terrorist and criminal groups move along this nexus spectrum in response to external pressures. She identified four aspects of interaction between criminal and militant groups: I. alliances, such as short- or long-term transactional partnerships; II. operational motivations, in which militants and criminals adopt each other's tactics for funding or logistical reasons; III. convergence, in which the aims of the two sets of actors or perhaps even the actors themselves merged; and IV. the "black hole" syndrome – i.e., the operating environment in which hybrid entities in weak or failed states capture state functions and perpetuate conflict for profit (Makarenko, 2004).

Similarly, Shelley and Picarelli argued that the crime-terrorism nexus progresses across stages: in the most basic form, the two sets of actors appropriate each other's methods without directly interacting with each other (Shelley, Picarelli, 2002). In the more complex forms, the two sets of actors interact and cooperate and form symbiotic relations. In the most advanced stage, according to Shelley and Picarelli, hybridization takes place, in which criminal and ideological objectives merge. Like Makarenko, the authors stress that groups can move fluidly along this spectrum in response to changing incentives and opportunities.

Across these models, scholars agree that terrorist and criminal organizations frequently exploit each other's financial, logistical, and territorial resources, blurring the traditional distinction between political and economic violence.

Felbab-Brown, however, emphasized that it is equally important to analyze when and how terrorist, militant, and criminal groups fight each other (Felbab-Brown, 2019). Understanding what puts them at odds and drives them apart is fundamental for designing effective policies toward the crime-terrorism nexus, she argues.

She also highlighted that pro-government militias also frequently collaborate with criminal groups and engage in illicit economies themselves, their (temporary) pro-government orientation not being any shield from their perpetrating criminal and nefarious activities (Felbab-Brown, 2010).

Indeed, the exploration of the crime-terrorism nexus has suffered from label problems – by being too narrowly focused on “terrorists” while ignoring a wide set of dangerous militant actors – be they insurgents or pro-government militias.

For decades, scholars, analysts, and governments have disagreed on the definition of terrorism and the application of the terrorist label to particular groups. Throughout the Cold War, one’s terrorist was another’s freedom fighter. Disagreements have persisted even among governments after the 9-11 al Qaeda terrorist attacks and post-911 global anti-terrorism regime. For example, only some governments have labeled the Taliban in Afghanistan, Boko Haram in Nigeria, Hamas in the Middle East, and the Revolutionary Armed Forces of Colombia (FARC) as terrorist organizations.

By designating more than a dozen criminal groups in Latin America as foreign terrorist organizations because they deploy intense violence, psychological intimidation, and target noncombatants, the Trump administration reflected an evolving approach in which the distinctions between criminality, militancy, and terrorism were further reduced. Various governments in Latin America, such as in El Salvador and Ecuador, and elsewhere in the world are also increasingly choosing to designate criminal groups as terrorist organizations, especially when the groups pose intense security challenges to the state.

This chapter does not seek to reopen the definitional debates. Instead, it embraces a broader concept of how criminality and militancy interact as the basis of the subsequent discussion of how emerging technologies and global trends will likely shape the nexus among different forms of violence.

Indeed, the intensifying political tendency of labeling aside, Felbab-Brown has identified three principal reasons of how terrorist/ militant groups and criminal organizations get together: I. They are pushed into the same physical space, such as weakly governed peripheries, by government actions against them. II. Terrorist and militant groups seek out criminal groups because they need their specialized skills or logistical networks, such as for financing, weapons acquisition, contraband and fighter movement, and money laundering. And III. Criminal groups need the firepower of terrorist groups to obtain protection from government actions against them.

Many of these motivations will weaken as both militants and criminals will be able to perform such services for themselves, across great distances, and with far fewer people.

From Territorial Control to Cyber-Enabled Operations across Great Distances

For decades, terrorist financing and operations were deeply tied to the control of territory. Territorial control provided access to resources, populations, and trade routes, as well as the coercive capacity to tax, extort, or manage illicit economies. Militant groups such as the Taliban, al-Shabaab, the DAESH, and the Revolutionary Armed Forces of Colombia (FARC) used land as both an economic base and a source of political legitimacy, especially when controlling land allowed for the employment of large populations in labor-intensive illicit economies (Felbab-Brown, 2010). Such territorial dominance allowed them to cultivate opium or coca, to levy taxes on commercial activity, and to regulate smuggling corridors in coordination with criminal networks. For instance, the Taliban's control over Afghanistan's poppy fields generated estimated annual drug-related profits in tens of millions, funding insurgent operations and embedding the movement within local communities (Felbab-Brown, 2013). Similarly, by extorting farmers, businesses, and even humanitarian organizations, al-Shabaab's territorial taxation in Somalia has been estimated to yield up to $100 million per year (U.S. Department of the Treasury, 2022).

Territorial control created not just an economic, but also a social infrastructure for criminal and militant groups and allowed them to function as governing entities (Felbab-Brown, Trinkunas, Hamid, 2017). Through local governance, justice administration, and intimidation, terrorist and insurgent groups created independent relationships with local populations and local government officials. This embeddedness - sometimes coercive only, other times underpinned by the provision of extensive services and employment to local populations - provided the organizational stability needed to manage extensive illicit economies and sustain prolonged campaigns of violence.

De-territorialized financing

Various emerging trends and technologies, such as the synthetic drugs revolution sweeping global drug markets and the proliferation of cybernetic networks, erode various advantages of territorial control, most importantly, the ability to generate money. Increasingly, financing activities can occur without physical presence or territorial governance across vast distances, many legal and law enforcement jurisdictions, and with low risk.

Instead of requiring vast territories, the *production of synthetic drugs*, such as methamphetamine and synthetic opioids, can be concentrated in the basements of several houses. Yet even such a small physical space, which can be dismantled, relocated, and recreated very rapidly, and the control of which takes only a few men, results in the production of highly dangerous drugs that can supply retail markets at a massive scale (Felbab-Brown, Caulkins, Humphreys, 2018).

Expanding *digital connectivity, the spread of artificial intelligence (AI), and the proliferation of cryptocurrencies* are transforming how illicit actors raise, move, and conceal money. More and more, AI-driven scams, cyber-enabled fraud, ransomware attacks, and cryptocurrency laundering will complement and eventually supplant traditional income streams.

AI has already begun to revolutionize criminal markets. Its integration into *online scams, identity theft, and social engineering* enables decentralized and highly adaptive fundraising mechanisms that can be perpetrated by very few across large distances and without any physical presence near their victims or tied to production sites.

Ransomware exemplifies the fusion of criminal and terrorist methodologies in cyberspace. It combines the coercive logic of hostage-taking with the financial efficiency of digital payment systems. Already, cryptocurrencies and virtual financial exchanges have been widely used to hide and move criminal proceeds. The current trend to deregulate them further will only increase the volume of illicit transactions.

The decentralized nature of cryptocurrency transactions will, in turn, enhance the capacity of malicious actors to conduct extortion across vast spaces without physical presence. During Russia's war of aggression on Ukraine, for instance, several ransomware operations appeared to operate in tandem with or parallel to military attacks, demonstrating how cyber infrastructure can serve both strategic and financial goals (National Cyber Security Centre, 2022).

Terrorist organizations could adopt similar tactics, using ransomware not only as a source of revenue but also as a weapon of disruption and intimidation.

AI will make such attacks more potent. Machine-learning algorithms can identify critical data or systems whose encryption would maximize leverage. Automated tools can scan networks for vulnerabilities, deploy malware, and negotiate payments through anonymized channels. As a result, ransomware operations will increasingly be conducted by autonomous or semi-autonomous AI agents, eliminating the need for human affiliates or intermediaries such as initial-access brokers (Geller, 2025). These developments lower the barriers to entry for cyber-enabled terrorism and complicate attribution and response through incapacitation and deterrence.

Similarly, money laundering has historically relied on human networks, couriers, corrupt officials, front companies, and professional facilitators. *AI and decentralized finance* (DeFi) are beginning to automate much of the money laundering process. Synthetic-identity generators and automated tools for creating cryptocurrency accounts can build complex laundering chains in minutes. Machine-learning models can design transfer routes across blockchains to maximize anonymity and minimize detection.

These innovations enable value to be moved globally without physical intermediaries or territorial infrastructure. For terrorist groups, this represents a paradigm shift. They can now receive donations, transfer assets, and pay operatives through decentralized platforms that operate beyond traditional financial oversight.

Empirical examples illustrate the trend. Between 2020 and 2025, analysts from TRM Labs identified nearly USD 3 billion stolen by North Korea–linked hackers, most of it through attacks on DeFi platforms (TRM Labs, 2025). DAESH supporters have also run online fundraising campaigns using Bitcoin, Ethereum, Monero, and Tron since at least 2019, soliciting donations via encrypted messaging applications(TRM Labs, 2025). Financial intelligence units report that between 2018 and 2022, 29 percent identified cases where virtual assets were linked to suspected illicit financing, activities, with funds directed to DAESH, Al-Qaeda, Hamas, , and the Al-Qassam Brigades (Egmont Group, 2023).

Crucially, donors increasingly send funds directly to individual or group wallet addresses rather than to centralized collection points in controlled territories. This mirrors the organizational decentralization of terrorist movements themselves: loosely connected cells, sympathizers, and virtual communities rather than unified, geographically defined structures.

Beyond raising money, emerging technologies can be used for other forms of infiltration by criminal groups. In 2024, the U.S. Financial Crimes Enforcement Network (FinCEN) issued an advisory warning that deepfake media were increasingly used to bypass “know-your-customer” protocols in financial institutions (U.S. Department of the Treasury, 2018). The same techniques can be employed by terrorist groups, especially those under sanctions or surveillance, to open accounts, move funds, and recruit personnel under false identities.

Current precedents already exist. North Korean IT workers, for example, have been documented using face-swapping technology during online job interviews to obtain legitimate remote employment, channeling the proceeds back to the regime (Financial Action Task Force, 2025). The convergence of AI and fraud thus allows sanctioned or isolated actors to access the global economy through deception.

Close-to- Home Logistics and Remote Attacks

Emerging technologies will also simplify various forms of logistical needs of terrorist and criminal groups, bringing close to their bases of operations many systems necessary for their operations.

For example, ever more effective *3-D printing and additive manufacturing will* reduce – and, for some groups perhaps altogether replace - the need to procure weapons in the illicit international market. Both criminal and terrorist groups will have the capacity to print even sophisticated weapons in the basement of their hideouts. Already, Brazilian criminal groups have developed the capacity to print high-power automatic rifles (Felbab-Brown, 2025). Advancements in 3-D printing coupled with AI will allow for the production of high-level fake biometric documents, such as passports, with the dispersion of this know-how and technologies equally available to both groups. Previously, even powerful militant groups, such as the DAESH, relied on international criminal groups, such as Brazilian ones, to acquire highly sophisticated passports to move their fighters from the Middle East around the world under newly acquired identities (Felbab-Brown, 2022).

Traditional bombs may still be desired by terrorist groups for their shock-and-awe intimidation effects and spectacular nature of violence. But a lot of killings and sabotage will not be dependent on them or on humans to physically deliver them. The increased availability and capacities of many remote platforms, such as cheap aerial drones, both military-grade proliferating from states and wars and modified off-the-shelf commercial ones, will allow killings and assassinations to be conducted from faraway places.

Both criminal and terrorist groups will be able to conduct assassinations, cause fatalities, and compromise critical infrastructure with the click of a button, such as by causing algorithms to malfunction. Assassinations could include *sabotaging individual vehicles or large-scale infrastructure systems*, such as air traffic control. With *the internet-of-things* connecting household appliances to such global networks, criminal and terrorist groups will be able to hack into in-house systems – internet-connected computers, TVs, vacuums, and other camera-furbished appliances to case out the joint for theft or to monitor the pattern of life of their victims.

But they will also be able to turn the household appliances into killing machines, rigging some to short-circuit to deliver a deadly electric bolt or to explode (Degeurin, 2026; Tucker, 2026; Neikirk, 2025; ID Watchdog, 2026). One day, skilled hackers working for states' espionage services or hackers working for militant or criminal groups will be able to reprogram in-house robots to kill their human families.

Cumulatively, being able to sabotage non-lethal systems into killing ones will give terrorist and militant groups a much-expanded scope of tactics and targets, especially when having a big bang of a large bomb going off somewhere is not the primary objective. But there will also be a great deal of psychological terror to be had out of the capacity to turn one's home, a presumed safe haven of security and privacy for ordinary citizens, into places of murder.

AI programs will assist criminal groups in discovering methods to hack and subvert such household systems for death. They will improve the production of bombs and biological weapons. Similarly, they will assist nefarious chemists to rapidly innovate the production of illegal synthetic drugs from new recipes from an ever-wider range of commonplace nonscheduled precursors. Such innovation will apply not just to the final analogs of known recreational drugs and their precursors but will also expand the speed with which entire classes of psychotropic drugs are being produced. Public health and law enforcement services may find themselves in a constant identification catch-up with what is arriving in the recreational and illicit markets.

In short, many more logistical needs and offensive actions will be accomplishable from a terrorist or criminal base far away without the need to rely on traditional illegal global supply markets.

Far Less Labor-Intensive Crime and Violence

Digital financing, remote platforms for trafficking and assassination, in-house production of contraband and kill systems, and subversion from faraway places will greatly reduce the need for fighters and other labor for both criminal and terrorist groups.

The territorial model of terrorist finance and criminal rule was labor-intensive. They required large-standing armies for the control of physical territories. The large labor forces also included those who ran shadow governorates, administered justice, collected taxes, managed logistics, and maintained military defense.

The AI systems and other emerging technologies will now allow groups to scale operations without proportional increases in manpower (Government of Canada, 2023). Automated scams, deepfake-enabled identity fraud, and algorithmic phishing campaigns can reach millions of victims at minimal cost. For example, Mexican criminal groups routinely embed accountants in many places of both legal and illegal extraction, harvesting, or seafood processing. With the threat of torture or death, they mandate that all producers only engage in harvesting when their accountant is present (Felbab-Brown, 2022a; Felbab-Brown, 2022b). Now, they will be able to simply insist that their CCTV cameras or other live-feed electronic systems are present at the place

of production, harvesting, extraction, or processing to assess their extortion fees-cum-taxation collection.

Even old-fashioned extortion and population control will become less labor-intensive and less anchored in land control. Instead of *halcones* (Mexican term for criminal lookouts) and al Shabaab sentinels in person watching retail markets for drugs or access roads to a town, drones, CCTV cameras (official ones hacked by the militant actors or ones specially installed by them), or personal cellphones will be usable to demand ransom and illegal taxes and control populations. Criminals or militants may demand that a person installs special app on their phone to subject themselves to their rule of being killed, just as the government of China demands that Uyghur people constantly run such apps on their phones even inside their homes (Human Rights Watch, 2019; Human Rights Watch, 2023).

Similarly, scam centers today enslave tens of thousands of people to lure and hook victims. Housing such large workforces has required entrapping those who would become forced entrappers themselves, hundreds of buildings to house the enslaved scammers, such as in the borderlands of China and Myanmar, food supply, and extensive coercion. In other words, running scam centers today takes a lot of labor and coercion.

Yet in a few years, deep-fakes will do away with the need to keep maintaining such large enslaved workforces. In several years, both criminal and militant organizations will use AI-driven tools to automate fraud and personalize deception at an unprecedented scale. Machine-learning algorithms can craft realistic messages and mimic human interaction, producing near-human-level phishing and social-engineering campaigns. For example, AI systems can analyze vast datasets, social-media profiles, transaction histories, or geolocation records to identify vulnerable individuals for exploitation (McKendrick, 2019). Deepfake technology further enhances these tactics. Synthetic audio and video can impersonate trusted figures or circumvent identity verification systems in banks and cryptocurrency exchanges (U.S. Department of the Treasury, 2024). Automated systems can simulate conversations, manage payment requests, and adapt to real-time detection. This automatization of fraud will reduce the demand for physical labor and further disengage fundraising from territorial or population control.

The changes in drug production provide another example. The cultivation of plant-based narcotic drugs often requires a very extensive labor force – tens of thousands or even hundreds of thousands of people in a locality, globally amounting to millions of people working in illicit drug production in the 2000s. The way synthetic drugs are produced reduces the labor requirements by several orders of magnitude – to mere thousands or even hundreds per locality.

The use of automated remote platforms for warfare and violence, and the ability to subvert commonplace everyday systems into tools of killing, will also drive a decreased dependence on physical forces for violence. Both terrorist and criminal groups will have the capacity to significantly shrink the sizes of their "armies" and fighter personnel. The *sicarios* too will be out of a job – at least the scores of low-skilled fighters, such as child soldiers and teenage criminals, while the tech-savvy operators will mete out death over large distances. Violent punishment for the failure to pay extortion fees may not come at the hand of an assassin who managed to come close to his victim, but from a kamikaze drone flown over tens of miles. In short, for both groups, conducting attacks and sabotage will become not just readily available across long distances, but also far less labor-intensive.

Sometimes, militant, terrorist, and criminal groups will choose not to transfer all of their ruling systems to automated machines. They may prefer to have a live-person shadow governor ruling a region and meting out justice decisions, not a virtual avatar. Perhaps they will trust the person more, or his or her physical presence may demonstrate the strength of their rule and their closeness to their subjects, in contrast to a distant state. But violent non-state armed actors will have the option of handling vast-population monitoring and administrative systems with far fewer people.

Overall, reducing the need for labor will not only allow militants and criminals to raise money more efficiently, but it will also allow many more actors – profit-motivated or ideology-motivated – to engage in illicit finance.

Less Labor, Less Political Capital

However, the reduction in the criminal and militant employment opportunities will also come with costs – most importantly, with significant reductions in political capital. Many criminal groups and militant groups obtain support from their members by providing them with employment when the legal economy and the government are not able to do so. This ability to employ people in the context of poor overall national economies, in labor-intensive economies such as drug cultivation or as fighters, also provided nonstate armed actors with a lot of political capital with local populations (Felbab-Brown, 2010). This political capital will be significantly reduced if crime and militancy are no longer sources of employment (Felbab-Brown, 2026).

If nonstate armed actors can raise enough illicit finance through cyberscams, for example, they may be able to offset some losses of such political capital through direct redistribution of the illegal gains – engaging in their own safety net handouts for those they no longer need to pay for illegal jobs.

At the same time, they will have a larger than ever pool of people from whom to recruit – not just low-skilled farmers, but also highly-educated programmers and tech specialists.

It is highly possible that the widespread adoption of AI will lead to massive unemployment, with scores of white-collar jobs made redundant and the skills of the fired workers not desired elsewhere. Not just youth, but middle-aged middle-class professionals may find themselves unemployed without official government safety nets.

Some may be employable by criminals. For example, programmers and IT specialists with high capacities to jailbreak AI systems and get them to provide information for illegal activities – such as making bioweapons or hacking into law enforcement systems and tracking the movements of law enforcement – that the systems are supposed to be prohibited from providing will have a bright future in crime and militancy.

Others may end up on the handout distribution systems of militants. Yet for some, even crime may not be an option. For centuries, criminality functioned as a survival option and a social pressure-release valve for those unable to join the formal legal economy. That option may disappear for many, leaving them to predatory banditry (Felbab-Brown, 2026).

The Value of Data and Data Security

If both territory and labor decrease in importance for nonstate armed actors, what will matter? The ability to acquire data, penetrate the data of rivals, and secure one's data from hostile breaches will be the critical assets. Particularly valuable learning data will matter for terrorists and criminals, so they, too, like everyone else, avoid AI slop.

The shift away from land and labor in crime and militancy will change the tools of coercion. Instead of controlling land and managing populations at the same scale, offensive and defensive operations will center on controlling digital infrastructure and manipulating information. The capacity to infiltrate systems, exploit data, and engineer digital trust will reduce the need to dominate physical spaces. Terrorist groups no longer need to secure villages or border checkpoints; they can instead compromise servers, cryptocurrency wallets, or communication platforms. One day, nonstate armed actors will be quite routinely able to hack satellites to steal data on populations or commercial trade or disrupt law enforcement operations. Already today, many commercial companies can penetrate satellites. The next big thing for nonstate armed actors will be sensor and processing integration.

The battle between security and law enforcement forces and personnel will center on competition over data control in a complex, contested, and transparent battlefield. The criminals and militants who will be able to spoof data, such as by sending out a false geolocation of their fighters or assets, and other false signals, or steal the electronic signatures of approved commercial drones to traffic contraband despite law enforcement efforts, will have a great edge.

Corrupting, intimidating, and recruiting the data guardians of governments, companies, and rival groups will become a premium focus of nonstate armed actors. Some of the intimidation and payroll recruitment of those who become insider threats may also become automated through deep-fakes, yet other may still entail an age-old human source skills such as physical seduction.

Equally, the most adept criminals and militants will also know which technologies, such as those prone to law enforcement sting operations, to stay away from while conducting business the old-fashioned manual in-person way.

This battle over public safety will inevitably entail highly contested and perhaps frequently changing public policy over data privacy. How much access to one's bedroom will publics be willing to relegate to governments, law enforcement forces, and tech companies to secure themselves from criminals and militants having access to their bedrooms?

Much Less Need for the Crime–Terror Nexus

The cumulative effect of these technological transformations is a weakening of the crime-terrorism nexus. A lot of cooperation between terrorists and criminals has stemmed from mutual material dependence: terrorists needed the logistical expertise of criminals, and criminals needed terrorists' protection. Digital tools now allow each to operate more autonomously and secure both types of essential operations for themselves on their own.

And avoiding falling in bed with each other also increases each group's operational security and reduces the chance of law enforcement infiltration by reducing the number of contact points with the outside world.

This does not mean that all convergence will disappear. Certain capabilities, particularly those requiring specialized technical skills or access to high-value data, may still encourage collaboration between terrorist and criminal actors. Some criminal networks may evolve into cyber mercenaries, offering top-level services such as malware development, ransomware infrastructure, dark-web marketplace access, superior-level AI jailbreaking, or hacking to terrorist clients.

Similarly, those with particularly highly-placed and widespread corruption networks in a region or functional domain will have unique advantages that cannot be easily replicated by machines. Selling access to their corrupt insiders may become a service that will continue connecting criminals and terrorists.

And, finally, just as state actions against criminal and terrorist groups simultaneously have often driven criminals and terrorists to alliances with each other up to now, such state actions will continue driving them together in the tech future. Joint forces against a common enemy in the form of a state or a rival nonstate armed actor will continue to bring advantages.

Yet, overall, the direction of the crime-terrorism nexus evolution is toward organizational fragmentation and functional self-sufficiency.

The Nexus with the State

Like in the past and the present, the criminal and militant groups that can obtain protection from a state will be at a great advantage. The crime-state and terror-state nexus will continue to outperform a crime-terror nexus as a source of danger.

State-linked nonstate armed actors will retain an advantage because, on average, an allied protector state will be capable of providing more sophisticated and extensive physical and digital safe havens, automated logistical and offensive platforms, algorithms, and valuable learning data than a nonstate armed actor. A nonstate armed actor in a nexus with a state, will be much better off than in a nexus with another type of nonstate armed actor. If the nonstate armed actors in a nexus with both a state and another nonstate armed actor type, will remain best off.

Which Territories Will Still Matter

Although both criminals and militants will be able to perpetrate a lot more illicit activity and violence without the need to control land than has been the case so far, not all land will lose value to them.

First, the identity of some militant groups and their objective may well be to govern large physical spaces and millions of people. Having a rebel state may be the very objective.

Second, having a physical safe haven, such as under the protection of a rival state, will still carry tremendous advantages. Beyond able to operate beyond the reach of law enforcement of a target country, such as Russian and Chinese hacker groups do today despite their attacks on Western infrastructure and systems, will be a critical asset. Not having to constantly look over one’s shoulder, not having to face the disruption of one’s personnel and physical asset networks will continue reducing the

need for asset replacement, simplify operations, and reduce psychological stress and exhaustion.

The physical protection of a sponsoring state will be especially useful since surveillance swarms will make hiding fixed assets such as terrorist training camps, smuggling depots, and extraction sites much harder for nonstate armed actors. Drug production sites or locations of additive manufacturing that will be cheap and thus easily abandoned with much cost, or conversely highly mobile, will be at a premium.

Third, with the coming proliferation of marine drones for the trafficking of contraband, the littoral where the marine – surface today, but eventually underwater too – will be able to dock and unload cargo, and people will be highly valuable real estate for criminals and militants too (Felbab-Brown, 2026). They may not need to control it on a constant basis and with a flag flying over that part of the coast, but they will need to secure access to the coast on a regular basis without running into law enforcement. Some territories will matter far more as sources of resource access than as places of permanent occupation.

And fourth, both the digital economy and digital crime and violence will depend on physical materials, physical data centers, and energy flows. For the foreseeable future, minerals, water, and energy will not be virtualizable. The infrastructure of digital life - from electric vehicles and renewable energy grids to cloud computing - depends on critical minerals such as lithium, cobalt, nickel, and rare earth minerals. The energy transition and the expansion of artificial intelligence, blockchain, and quantum computing will amplify the demand for these materials. Already now, data centers require vast amounts of water and energy. By 2040, securing access to critical minerals, water sources, and cheap secure energy production will be as strategically significant as controlling oil fields once was.

Control of these physical territories with these tangible assets will remain an enduring priority for governments and their nonstate armed rivals. At the same time, technological advances in surveillance and weaponry will radically alter what “holding” territory means. Territory will persist, but in more fluid, adaptive, and high tech-forms.

Yet many regions of the world that today are weakly governed and conflict-prone regions are and will likely remain the primary sources of these critical minerals. Terrorist and criminal groups are therefore likely to replicate the predatory political economies that currently surround illicit gold mining (International Crisis Group, 2019). They will extort local miners, take over extraction and smuggling routes, and control artisanal and small-scale mining sites where state presence is minimal. The experience of groups like the DAESH or the Wagner Group/Africa Corps proxies in Africa foreshows how mineral-rich territories can become self-financing war economies. As mineral frontiers expand, so will the intensified competition between

state-backed militias, private security actors, and hybrid terrorist-criminal entities seeking to dominate extraction zones and trade corridors. The capacity to control these “material chokepoints” will translate into sustained sources of revenue and leverage in both local and transnational markets, and the ability to conduct crime and violence.

With as much as three-quarters of the world’s population estimated to live in areas of severe water stress by 2024, increasing water scarcity will concentrate areas of water availability and make them a desired target for all, including nonstate armed actors (Office of the Director of National Intelligence, 2021). Criminals and militants may make seek to control water sources and supply to disrupt the digital functioning of their rivals. Or they may use control of water as an ideological propaganda tool, like Robin Hoods, taking water away from large, affluent, greedy international tech companies and handing it out to local populations struggling to source water for drinking and food production. And they may profit from running large-scale local and even international water trafficking economies (Felbab-Brown, 2017).

Cutting off water from large data centers and otherwise attacking and disrupting large data centers will allow nonstate armed actors to bring down the functioning of large parts of the global economy and public safety systems.

Controlling or sabotaging these nodes will become a new form of territorial competition, not just among states, but also between them and nonstate armed groups. Actors that dominate local data infrastructure could monitor populations, intercept communications, and even disrupt the cyber operations of their rivals or state opponents. Safety of such centers and of key strategic processing headquarters will thus be key objective of governments and law enforcement.

Yet the 2026 Iran war showed how cheap remote automated platforms (currently in the hands of states, but soon in the hands of many nonstate armed actors) can make such critical infrastructure vulnerable. Building multifaceted anti-drone defenses and developing mechanisms to overcome and penetrate them will be a core element of competition between states, terrorist groups, and very ambitious criminal organizations.

Some territories will thus function not merely as a space to inhabit, but as economic substrate and platforms for taxation, labor control, and resource monopolization, and a source of crucial advantage.

When nonstate armed actors desire to seize some territories, emerging technologies will transform how terrorist and criminal groups take them and hold them. The proliferation of autonomous surveillance and strike systems will render territorial control both more visible and more volatile. Both criminals and militants will

increasingly deploy autonomous drones (airborne, land-based, maritime, and subaquatic) acquired through grey markets, state sponsorship, or 3D printing (Hartzell, 2023). Equipped with AI-enabled facial and thermal recognition, these systems will execute surveillance, targeting, and attacks with minimal human oversight. Drone swarm coordination, allowing dozens of drones to share data and conduct synchronized maneuvers, will replace much of today's human reconnaissance and combat operations – for conventional armies and nonstate armed actors (Hartzell, 2023). Drones equipped with laser weapons will enable strikes on checkpoints, convoys, or infrastructure, undermining conventional defenses.

The purpose of territory will thus be transformed: For some terrorist and criminal organizations, the value of territory will lie less in static governance and more in its capacity to generate, protect, or manipulate strategic resources.

Conclusions

Over the next two decades, violence by nonstate armed actors, criminality, and illicit economies, as well as terrorist groups and criminal organizations will all change. And so will the nexus between organized crime and terrorism. Violence and organized crime will both become far less dependent on physical territories for generating operational revenues and profits and far less labor-intensive.

And many of the incentives that drove criminals and politically-motivated terrorist groups together will no longer be present. Specialist logistical networks of smuggling, sought-after contraband such as weapons and top-level forgery documents, and production of high-value assets will become dispersed and move closer to the home base of terrorists. For example, they will be able to use additive manufacturing for producing weapons such as drones and rifles. And criminal groups will far less need terrorist groups for physical protection.

Similarly, within a matter of years, terrorist and criminal groups will no longer need to rely on controlling territories, populations, and labor-intensive economies for conducting business – though some may choose to do so because running a rebel state is their primary objective. But they will have the option to exploit digital infrastructures such as networks, data, and algorithms to generate financial resources through AI-enabled scams, ransomware attacks, cryptocurrency money laundering.

Criminality and rebellion will similarly evolve toward being far less dependent on many fighters and other employees, such as farmers of illicit crops, toward algorithmic exploitation of data vulnerability. Even extortion, which for many criminal groups drove the need to control physical spaces and exclude rivals, will become far less dependent on physical control and carried out digitally.

Remote platforms such as drones as well as the cyber-sabotage of everyday household appliances and cars will allow both crime and any kind of violence, including assassinations and territorial takeover, to be conducted over great distances by a few people. Sabotaging non-lethal systems such as household items into means of surveillance, expropriation, and death will give terrorist and militant groups a much-expanded scope of tactics and targets and an enhanced ability to generate psychological terror.

These processes will culminate in a de-territorialized fundraising, operating, and violence systems. In some cases, terrorists and criminals will also become far less dependent on physical territories for accomplishing and facilitating many of their objectives– including the ability to conduct attacks, raise money for their operations, and procure weapons. Violent and non-violent crime as well as militancy will be able to take place without physical presence or territorial governance across vast distances and many legal and law enforcement jurisdictions.

But there will also be costs to the de-territorialization and reduced labor-intensivity of crime and violence. Both groups will be able to provide far less employment to those unable to participate in the legal economy at a time when AI adoption will likely drive vast increases in unemployment around the world. By hiring fewer people, criminals and militants will lose significant political capital.

Data and data security will become the biggest prize. The ability to acquire valuable data, such as learning data, to penetrate the data of rivals and spoof it, and to secure one's data from hostile breaches will be the critical assets. Corrupting, intimidating, and recruiting the data guardians of governments, companies, and rival groups will become a premium focus of nonstate armed actors, whether through AI-driven deep-fakes or old-fashioned in-person intimidation and seduction. The battle between security and law enforcement forces and personnel will center on a competition over data control in a complex, contested, and transparent battlefield. Yet public policies may struggle to balance citizens' privacy with public safety.

The dispersion of knowledge and smuggling and killing systems does not mean that all incentives for the crime-terrorism nexus will go away. Certain capabilities, particularly those requiring specialized technical skills or access to high-value data, may still encourage collaboration between terrorist and criminal actors. And state actions against criminals and insurgents may drive them together in the future as they have done over many decades.

But the ability to align one's group with a state and obtain its support and protection will outperform a crime-terror nexus. On average, a protector state will be able to provide a nonstate armed actor will better data, algorithms, automated logistical and offensive platforms, and physical and digital protection.

The ability to enjoy a safe haven provided by another state and thus physical protection from the reach of law enforcement and security forces of other countries is one reason why not all territory will decline in value. Another reason is that the digital economy and crime and violence in the digital era will still depend on physical materials, physical data centers, and energy flows. The capacity to control these "material chokepoints" of data production, the data centers themselves, and headquarters of data synthesis will translate into sustained sources of revenue and leverage in both local and transnational markets, and the ability to conduct crime and violence. Littoral areas will be another type of highly desirable territory, functioning as a crucial node of smuggling once marine drones proliferate.

Recommendations for NATO

The policy implications and recommendations from this policy analysis fall into two categories: One is a good practice toward upcoming forms of criminality and politically-motivated violence, irrespective of whether these two interact with each other. The second type focuses specifically on the nexus between the two. They include:

1. Investing heavily in the protection of one's data and developing mechanisms to infiltrate and penetrate data systems of nonstate armed groups and deprive them of their critical infrastructure assets;
2. As much as possible, controlling and tracking modern systems of weapons production, such as 3D printers and other forms of additive manufacturing;
3. Building strong defenses around one's data centers and supply of critical minerals, water, and energy while making sure that populations remain equitably able to access such vital resources;
4. Encouraging private companies to build in the best possible security systems to avoid hacking, including into everyday common appliances and household items such as cars and minimizing the commercial distribution of personal data, such as from rental cars or websites;
5. Incentivizing private companies to share information about hacks and sabotage coming from criminals or militants with government authorities;
6. Motivating and enabling individual citizens as well as companies to adopt best data security practices;
7. Building strong public trust foundation for the balance of data privacy and law enforcement digital access while maintaining a steadfast commitment to human rights, civil liberties, and democratic accountable processes;
8. Hardening one's networks against insider threats;
9. Countering state sponsors of terrorism and criminality;
10. Providing safety nets for the many who will be rendered unemployed or unemployable by AI and other modern technologies; avoiding operations that inadvertently push militant and criminal groups together;

11. Devising operations to push the two actors apart and turn them against each other such as through law enforcement or intelligence services run deep-fake and sting operations to sow distrust between the two sets of actors; and
12. Hunting for digital vulnerabilities in the nexus and recruiting soft assets from within it.

Countering criminality and politically-motivated violence and the nexus between the two will become far more challenging. But law enforcement and security forces too will have access to the very same technologies, and if they manage to adopt them speedily as well as in an accountable manner will remain potent opponents to nonstate armed actors.

References

Degeurin, Mark. (2026) 'Man accidentally gains control of 7,000 robot vacuums,' *Popular Science*, February 21, 2026. https://www.popsci.com/technology/robot-vacuum-army/.

Egmont Group (2023) 'Abuse of virtual assets for terrorist financing purposes (IEWG Project),' July, 2023. https://www.egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf.

Felbab-Brown, Vanda. (2010) *Shooting up: Counterinsurgency and the war on drugs*. Washington, DC: The Brookings Institution.

Felbab-Brown, Vanda. (2011) 'Human security and crime in Latin America: The political capital and political impact of criminal groups and belligerents involved in illicit economies'. FIU/WHEMSAC, September, 2011. https://digitalcommons.fiu.edu/whemsac/40/.

Felbab-Brown, Vanda. (2013) *Aspiration and ambivalence: The strategies and realities of counterinsurgency and state building in Afghanistan*. Washington, DC: The Brookings Institution.

Felbab-Brown, Vanda. (2017) 'Water theft and water smuggling: A growing problem or tempest in a teapot?'. The Brookings Institution, March, 2017. http://brookings.edu/wp-content/uploads/2017/03/fp_201703_water_theft_smuggling.pdf.

Felbab-Brown, Vanda. (2019) 'The crime-terrorism nexus and its fallacies', in Chenoweth, E., English, R., Gofas, A. and Kalyvas, S.N. (eds) *The Oxford Handbook of Terrorism*. Oxford: Oxford University Press.

Felbab-Brown, Vanda. (2022a) 'China-linked wildlife poaching and trafficking in Mexico'. The Brookings Institution, March, 2022. https://www.brookings.edu/research/china-linked-wildlife-poaching-and-trafficking-in-mexico/.

Felbab-Brown, Vanda. (2022b) 'How do we resist? – Organized crime is taking over Mexican fisheries – Part II', *Mexico Today*, March 6, 2022.

https://mexicotoday.com/2022/03/06/opinion-how-do-we-resist-organized-crime-is-taking-over-mexican-fisheries-part-ii/.

Felbab-Brown, Vanda. (2026) 'How Mexican cartels are using drones, now and in the future'. The Brookings Institution, 19 February, 2026. https://www.brookings.edu/articles/how-mexican-cartels-are-using-drones-now-and-in-the-future/.

Felbab-Brown, Vanda. (2025) Interviews with Brazilian law-enforcement officials, August.

Felbab-Brown, Vanda. (2022; 2024) Interviews with Brazilian and U.S. law-enforcement officials, June 2022 and September 2024.

Felbab-Brown, Vanda. and Paz García, Diana. (2024) 'Russia, Ukraine, and organized crime and illicit economies in 2024'. The Brookings Institution, February 6, 2024. https://www.brookings.edu/articles/russia-ukraine-and-organized-crime-and-illicit-economies-in-2024/.

Felbab-Brown, Vanda., Caulkins, Jonathan. and Humphreys, Keith H. (2018) 'How synthetic opioids can radically change global illegal drug markets and its international relations implications'. The Brookings Institution, May, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/04/30/how-synthetic-opioids-can-radically-change-global-illegal-drug-markets-and-foreign-policy/.

Felbab-Brown, Vanda., Trinkunas, Harold. and Hamid, Shadi. (2017) *Militants, criminals, and warlords: The challenge of local governance in an age of disorder*. Washington, DC: The Brookings Institution Press.

Geller, Eric. (2025) 'AI-fueled automation helps ransomware-as-a-service groups stand out from the crowd', *Cybersecurity Dive*, October 21, 2025. https://www.cybersecuritydive.com/news/ai-automation-ransomware-affiliates/803362/.

Government of Canada, Department of Finance Canada (2023) *Updated assessment of inherent risks of money laundering and terrorist financing in Canada*. March, 2023. https://www.canada.ca/en/department-finance/programs/financial-sector-policy/updated-assessment-inherent-risks-money-laundering-terrorist-financing-canada.html.

Hartzell, Christopher L. (2023) 'Future weapons technology of 2040', *NCO Journal*, July 10, 2023. https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2023/July/Future-Weapons-Technology-of-2040/.

Human Rights Watch (2019) 'How mass surveillance works in Xinjiang, China: Reverse engineering "Police App" reveals profiling and monitoring strategies', May 2, 2019. https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang.

Human Rights Watch (2023) 'China: Phone search program tramples Uyghur rights', May 4, 2023. https://www.hrw.org/news/2023/05/04/china-phone-search-program-tramples-uyghur-rights.

ID Watchdog (2026) ‘The FBI warns that smart TVs can be a gateway for hackers to enter victims’ homes’, *ID Watchdog*, March 29, 2026. https://www.idwatchdog.com/education/-/article/smart-tv-hackers.

International Crisis Group (2019) *Getting a grip on Central Sahel’s gold rush*. Africa Report no. 282, November 13, 2019. https://www.crisisgroup.org/sites/default/files/282%20Getting%20a%20Grip%20.pdf.

Makarenko, Tamara. (2004) ‘The crime-terror continuum: Tracing the interplay between transnational organised crime and terrorism’, *Global Crime*, 6(1), pp. 129–145.

McKendrick, Kathleen. (2019) ‘Artificial intelligence: Prediction and counterterrorism’. Research paper, International Security Department, Chatham House, August, 2019. https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf.

Neikirk, Lee. (2025) ‘How to get your smart TV to stop spying on you’, *New York Times (Wirecutter)*, October 6, 2025. https://www.nytimes.com/wirecutter/reviews/can-smart-tvs-spy-on-you/.

Office of the Director of National Intelligence (2021) ‘The future of water: Water insecurity threatening global economic growth, political stability’, March, 2021. https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-water.

Rogers, J. (2022) ‘The third drone age: Visions out to 2040’. Centre for International Governance Innovation, November 28, 2022. https://www.cigionline.org/articles/the-third-drone-age-visions-out-to-2040/.

Shelley, Louis.I. and Picarelli, John T. (2002) ‘Methods not motives: Implications of the convergence of international organized crime and terrorism’, *Police Practice and Research*, 3(4), pp. 305–318.

TRM Labs (2022) ‘Fundraising campaigns for ISIS families: Analysing the use of cryptocurrency’, April 11, 2022. https://www.trmlabs.com/post/fundraising-campaigns-for-isis-families-analyzing-the-use-of-cryptocurrency.

TRM Labs (2025) ‘US Treasury sanctions North Korean cyber facilitator linked to IT worker scheme’, *TRM Blog*, July 7, 2025. https://www.trmlabs.com/resources/blog/us-treasury-sanctions-north-korean-cyber-facilitator-linked-to-it-worker-scheme.

Tucker, Sean. (2026) ‘Explaining the car “kill switch” controversy’, *Kelley Blue Book*, January 26, 2026. https://www.kbb.com/car-news/explaining-the-car-kill-switch-controversy/.

U.S. Department of the Treasury (2022) ‘Treasury designates al-Shabaab financial facilitators’. Press release, October 17, 2022. https://home.treasury.gov/news/press-releases/jy1028.

U.S. Department of the Treasury, Financial Crimes Enforcement Network (2024) ‘FinCEN issues alert on fraud schemes involving deepfake media targeting financial institutions’. Press release, November 13, 2024. https://www.fincen.gov/news/news-

releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial.

Williams, Phil. (2012) ‘Transnational organized crime’, in Williams, P.D. (ed.) *Security studies: An introduction*. London: Routledge, pp. 503–520.

CHAPTER 6

Terrorists with Drones:

Exploring the Effects of Lethal Autonomy on the Future of Counterterrorism

Prof. Dr. Giray Sadık

Abstract

The proliferation of drone-related technologies has amplified growing concerns about the emerging threats from the terrorist possession and exploitation of drones. Considering the combination of asymmetrical advantages of drones and ease of access to related Emerging and Disruptive Technologies (EDTs), terrorists are likely to use drones more in the forthcoming years. This worrying trend underscores an urgent need for deeper reflection about how the counterterrorism community should adapt to this emerging threat landscape, where Artificial Intelligence (AI) and Lethal Autonomous Weapons Systems (LAWS) have become increasingly available to both state and non-state actors. Combined with the recent drone-related innovations from the Russia-Ukraine War, it can be foreseen that the terror drone landscape is poised for another eruption akin to the 9/11 terrorist attacks that may come sooner than expected in part because of the growing availability of battle-hardened fighters and tactics from Ukraine to MENA. To mitigate these risks, the forthcoming counterterrorism strategies must adapt to the changing landscape of warfare. Key measures include, but not limited to, enhancing drone defense systems and investment in anti-drone technologies. These necessary adjustments to technological developments put forward the need for multi-stakeholder reflection by the counterterrorism community, so that the lessons learned can be followed by timely strategic adaptation.

Introduction

Drone is an umbrella term for remote-controlled (via operator and/or AI) platforms such as Unmanned Aerial Vehicles (UAV), Unmanned Ground Vehicles (UGV), Unmanned Surface Vehicles (USV), and Unmanned Underwater Vehicles (UUV) that operate without a pilot onboard. In the past such advanced technologies have been available to only a few developed states. The recent proliferation of drone-related technologies (e.g. GPS, FPV, etc.) has amplified growing concerns about the emerging threat from the terrorist possession and exploitation of drones. As Major Thomas G. Pledger from U.S. Army observes “the most prescient current technology that will *enable future*

terrorist attacks is the drone. Drones have the ability of providing standoff, which can enable terrorists to conduct multiple attacks nearly simultaneously, rapidly magnifying their overall effect" [*italics added for emphasis*] (Pledger 2021). Considering the combination of asymmetrical advantages of drones and ease of access to related technologies, terrorists are likely to use drones more in the forthcoming years. This worrying trend underscores an urgent need for deeper reflection about how the counterterrorism community should adapt to this emerging threat landscape, where Artificial Intelligence (AI) and Lethal Autonomous Weapons Systems (LAWS) have become increasingly available to both state and non-state actors.

To address these challenges, this chapter adopts a forward-looking perspective on the evolving relationship between drone technologies, terrorism, and counterterrorism. It begins with an introduction and discussion of the current security landscape before examining the growing threat posed by the terrorist use of drones and the potential trajectory of these capabilities. The chapter then assesses the role of drones in counterterrorism, considering whether their expanding capabilities represent a genuine strategic advantage or create new operational and ethical risks. Particular attention is given to the threats posed by terrorist drone use against Türkiye and NATO, followed by an analysis of emerging trends associated with Lethal Autonomous Weapons Systems (LAWS). Building on these discussions, the chapter explores future technological advancements and their implications for NATO allies and partners. It concludes by offering key findings alongside policy recommendations aimed at strengthening preparedness, resilience, and collective security in the face of rapidly evolving drone-enabled threats.

Rising Threats from Drone-Terrorism: How far can they go?

Will terrorists use drones? is not an *if*, but rather *how* and *when* type of a question. The process is already underway in the Middle East, and its pace is growing at an unprecedented speed since the outset of the Russia-Ukraine War. Several experts note that "the Russo-Ukrainian War has become a critical 'innovation hub' for drone warfare, accelerating advancements in the scale, speed, and range of drone operations. Can you describe these advancements in scale, speed, and range of drone operations as seen in Ukraine?

These developments are not only transforming the modern battlefield but also creating new opportunities for violent extremist organizations (VEOs)" (Rassler and Veilleux-Lepage 2025). Evidently, terrorists are already on this learning curve, as "the massive increase in the number of form factors, capabilities, ease of access and ease of operation of drones at low cost makes them the weapon of choice for future terrorists" (Pledger 2021). For example, "the widespread use of high-speed First-Person View (FPV) drones in Ukraine highlights the tactical value of speed and agility —capabilities that are *increasingly within reach for terrorist actors*. When paired with

emerging technologies such as AI-assisted targeting, these systems could significantly increase the precision and impact of future attacks" [*italics added for emphasis*] (Rassler and Veilleux-Lepage 2025).

When exploring the rising threats from drone-terrorism, we need to keep in mind that terrorists are not passive observers in modern warfare, but they aggressively monitor, investigate, and incorporate military advancements into their own strategies. Considering these lessons learned from the warzones like Ukraine, Yemen, Syria, etc. terrorists constantly update their objectives and seek the related capabilities. For example, according to recent reports:

> Several terror networks have been 'eyeing' and appear to be actively working to acquire or develop commercial UAS, or related technology, that will enable them to elongate range and strike from further afield. Of particular concern in this regard is the discovery off the coast of Yemen of what is believed to be parts of a commercial hydrogen fuel cell tied to the Houthis. The case illustrates how ongoing advancements in UAS technologies and related systems that affect range are going to compound other C-UAS [Counter-Unmanned Aerial Systems] challenges. (Rassler and Veilleux-Lepage 2025)

Looking ahead over the next 20 years, where do we think terrorists and/or terrorist organizations will acquire drones? And from whom? Will it be some A.Q. Khan character? Will they develop them on their own, like the Iraqi insurgents did with IEDs? What are the cost factors to consider? Are costs for drones and drone tech going down? Traceability?

What obstacles will terrorist groups be confronted by over the next 20 years in their effort to acquire drone technology and components?

Terrorists' desire to utilize UAS (Unmanned Aerial Systems) to attack from greater stand-off distances is likely to grow, as the greater the distance the more difficult to be detected and the UAS-technologies have become more commercially available. The proliferation of drone-related technologies is likely to fuel dual-use problems like the ones related to nuclear technologies. Nevertheless, such dual-use drone-technologies challenges are likely to be more difficult to handle with non-state actors such as terrorists. Moreover, adding to this greater stand-off, terrorists work to increase the number of drones used to attack, making them more difficult to intercept, and thus to attack civilians and military targets via *drone swarms*. There are growing concerns that drone swarms could significantly increase the impact of terrorist drone

operations, be it kinetic strikes, ISR (Intelligence, Surveillance, Reconnaissance), or psychological warfare:

> Drone swarms, the coordinated use of drones with minimal human intervention using algorithms and sensors, can range from just a few to over thousands. Coordinated drone swarms operate with real-time communication, often employing artificial intelligence for predetermined flight paths and are controlled by a central operator. Drones have been used in a variety of operations, ranging from bomb-drop strikes, ISR missions, artillery guidance, and kamikaze attacks. This is likely just the tip of the iceberg. As drone swarms and artificial intelligence technologies increase and continue to develop in tandem with one another, both state militaries and VNSAs [Violent Non-State Actors] will likely develop new capabilities and tactics. (Rassler and Veilleux-Lepage 2025)

Evidently, when asking about *how far they can go?* it seems that *the sky is the limit* for terrorists and drones are expanding this threat horizon beyond our imagination. Simply put, “the ability of a small group or individual to conduct multiple simultaneous attacks, at a relatively low cost and with significant standoff distance, will lead to the *use of drones as a primary tactic of future terrorist attacks*” [*italics added for emphasis*] (Pledger 2021). Therefore, with no end in sight about the distance they can travel, it is only a matter of time before we see another *9/11-moment with drones*. Under these circumstances, where drones further complicate the prevention of terrorist attacks, it is time to have a sober reflection on how to use drones effectively for counterterrorism.

Before launching into how to use drones effectively for counterterrorism can we describe a range of possible use cases of terrorist drone attacks against NATO targets? What might be the softest targets? Which would be the most symbolically effective targets? The brief discussion of swarms might be expanded with a description of the added effectiveness and exponentially increasing threat posed by drone swarms.

Drones for Counterterrorism: Growing Capability or Lethal Illusion?

Armed drones are designed to identify, surveil, and engage targets with kinetic weapons, hence their increased use in global counterterrorism efforts, a trend that is likely to grow. For instance, “the United States has significantly increased its use of armed drones to attack global counterterrorism targets since the terrorist attacks of September 11, 2001, continuing to today to support U.S. and partnering country counterterrorism missions” (Rollins 2023). For example, this trend of drone surveillance has been effective especially in recent CT-operations in the Middle East

including, but not limited to, the targeting of prominent figures (Organizations' name in the following parentheses) such as Anwar al-Awlaki (AQ), Ayman al-Zawahiri (AQ), Qasem Soleimani (IRGC), Baitullah Mehsud (TTP), and Abu Musab al-Zarqawi (AQI). In addition to the United States, this trend is likely to demonstrate growing use among other NATO Allies, while harboring the risk of being used effectively by terrorists against NATO Allies and Partners. There are two underlying reasons that can be identified behind this growing trend of drone use for counterterrorism: "the *drone contributes to the counterterrorism mission* by providing pervasive intelligence and aggressive strike capabilities … [that] hinder the operational capacity of the terrorist organization by eliciting fear, fracturing communication, and decimating command and control" [*italics added for emphasis*] (Farrow 2016). What is the second underlying reason?

Increasingly, drone strikes have become the preferred option for counterterrorism missions by the United States and other NATO Allies dealing with terrorism such as Türkiye, offering a range of capabilities from surveillance to kinetic strikes:

> Drones perform a variety of national security missions for the United States. Specific to how *armed drones support counterterrorism missions*, the following are commonly performed functions:
>
> • *Identifying High-Value Targets*: conducting ISR to identify terrorist leaders or those possessing special skills deemed to be a significant threat to the United States. Operators can use both armed and unarmed drones for such a mission.
>
> • *Executing Signature Strikes*: lethally targeting unidentified individuals based on behaviors, patterns, and locations often associated with terrorist organizations.
>
> • *Targeting Equipment/Facilities*: destroying buildings or training areas used to house or support terrorist activity. [*italics added for emphasis*] (Rollins 2023)

These critical capabilities of drones for American counterterrorism efforts have paved the way for the growing use of drones by NATO Allies suffering from terrorist attacks such as the UK, Türkiye, and Spain. As a result, there is an emerging defense-industry-ecosystem of drone-production and deployment among growing number of Allies to better harness the capabilities of drones for counterterrorism ranging from *AI-assisted-targeting* to the development of Counter-Unmanned-Aerial-Systems (C-UAS) technologies.

On the one hand, it is promising that this is a growing trend among NATO Allies in addition to the United States. On the other hand, the proliferation of drone-related technologies has brought risks of their development by regional and global competitors such as Russia, China, and Iran. For example, recently “we are already witnessing the emergence of advanced deep-strike drones, such as Iranian Shahed drones used by Russia” (Liang 2025, 1). Both trends are likely to grow in tandem with the increasing use of drones in ongoing clashes in Ukraine, MENA, etc. with the potential to lead a new generation arms-race in drone technology, under the guise of counterterrorism.

Although, drones have been a preferred surveillance tool and strike platform for a growing number of counterterrorism actors, “significant concerns remain regarding the decision to deploy them in future counterterrorism operations. RPAs [Remotely Piloted Aircraft] have caused collateral civilian casualties, eroding U.S. legitimacy and providing cause for recruitment into extremist organizations. Without an on-the-ground presence, the possibility of inadequate intelligence and misanalysis could further undermine the effectiveness of RPA-based OTH-CT [Over-The-Horizon-Counter-Terrorism] missions” (Yayboke and Reid 2022). These critical issues deserve a thorough consideration when deploying drones for counterterrorism to prevent this growing CT-capability to turn into a lethal illusion of effective counterterrorism. In the next section, I expand the discussion on how the proportionality, military necessity, and Emerging Disruptive Technologies (EDTs) factor in the counterterrorism efforts of NATO Allies targeted by various terrorist groups such as Türkiye.

Threats from Terrorists-use of Drones against Türkiye and NATO

For Türkiye, the next 20 years (2026–2046) present a paradoxical landscape: the nation is a global drone-superpower, yet its geography and the evolution of its adversaries make it increasingly vulnerable to the very technology it helped pioneer. As we look toward 2046, the Third Drone Age will bring threats that are increasingly autonomous, stealthy, and difficult to attribute. One of the concrete examples of “the terrorist organization’s [PKK] tendency to use drones. Records show that drones played an important role in the actions carried out by the organization. On the other hand, the PKK’s start of drone-based actions has resulted in Türkiye increasing its investments in *anti-drone systems*” (Özgen and Kurt, 2025). As illustrated in the below Table-1, the defensive roadmap of Türkiye aims to harness EDTs such as drones, AI, lasers, C-UAS systems, etc. keep its edge against growing terrorist and hybrid threats in its neighborhood.

Table-1: Defensive Roadmap of Türkiye (2026–2046)

Technology	Purpose
Directed Energy (Lasers)	Using systems like **ALKA** to destroy drone swarms at the "cost of electricity" rather than expensive missiles.
AESA Radar Expansion	Deploying "Low-Altitude Radar Links" along the entire Syrian and Iraqi borders to detect drones as small as a bird.
AI-Counter Drones	Deploying "Interceptor Drones" (like STM's **KARGU** in a defensive role) that hunt and crash into hostile drones autonomously.

Because Türkiye is a leading developer and exporter of advanced drone technologies, operating at the forefront of a rapidly evolving security environment, which—like in all cases involving advanced defence capabilities—brings potential risks related to the unintended proliferation and adaptation of such technologies. In the next 20 years, components or designs from drones used across different operational environments could be reverse-engineered or captured by extremist groups, who then use similar tactics against state forces. Increasing accessibility of unmanned aerial systems (often referred to as the "democratization of air capabilities") means that by 2040, the air superiority in operations against non-state actors may become increasingly contested. The operational focus is likely to shift more prominently to the low-altitude layer (0–500 meters) as a critical domain. While these risks can be viewed, as particularly relevant in Türkiye's context the lessons from Allied CT-efforts demonstrate that terrorists are fast in learning and adopting new tactics from each other. Therefore, developments in Türkiye's operational environment may have broader implications for the future of NATO and global counterterrorism strategies, including but not limited to, the following growing threats from terrorists' drone use:

- *Energy Infrastructure:* Türkiye's ambition to be a regional energy hub makes its pipelines and refineries prime targets. A drone "swarm" attack on the TANAP pipeline or offshore gas platforms in the Black Sea could cause billions in damage and long-term economic instability.

- *The "Border Gap":* Despite the "security wall" and advanced sensors, the sheer length of the Syrian and Iraqi borders remains a challenge. Terrorist groups could use heavy-lift cargo drones (capable of carrying 50–100kg) to smuggle weapons, explosives, or people over the border, bypassing ground-based patrols entirely.

- *Psychological Operations (PsyOps):* Drones equipped with high-powered loudspeakers or projectors may be used to disrupt public gatherings or spread propaganda in real-time during sensitive periods, such as elections.

- *Urban Terrorism and "Dark Drones":* Small drones provide an easy delivery vector for non-conventional weapons (e.g. CBRN) over crowded public squares or stadiums, where traditional security checkpoints are ineffective.

- *3D-Printed "Ghost" Drones:* By 2040, the widespread availability of industrial 3D printers will allow cells to manufacture drones entirely within Türkiye using non-metallic carbon fibers, making them nearly invisible to conventional radar and impossible to track through supply chains.,

- *Precision "Assassination" Drones:* Moving away from bulkier commercial quadcopters to miniature, high-speed FPV (First-Person View) drones that can navigate through windows or open doors of government buildings and military outposts in the Southeast.

- *Loitering Munitions as Artillery:* Groups could likely acquire or "emulate" loitering munitions (suicide drones) capable of flying 50–100 km behind Turkish lines to target supply convoys, fuel depots, and high-value personnel.

- *Trench-to-Drone Integration:* In border regions like Northern Iraq and Syria, drones will become the primary "eyes" for every insurgent squad, making it nearly impossible for Turkish units to maintain the element of surprise during ground operations.

- *Swarm Intelligence:* By the 2030s, the greatest threat to Türkiye's critical infrastructure will be Saturation Attacks. Terrorist groups, potentially backed by state actors (proxies), will utilize AI-driven swarms.

Looking Ahead: Emerging Trends and Challenges from LAWS

The growing use of drones by terrorists underscores three main trends and interrelated challenges that need sober assessment concerning the role of drones in counterterrorism efforts. First, it is the fact that must be recognized: "*the advantage is with the attacker*; expensive counter systems for drones can be defeated with the addition or removal of specific onboard systems or a change in modality. Terrorists have already begun to experiment with the use of drones in their attacks —it would only take one high-profile attack for all terrorist groups to realize and exploit this technology" [*italics added for emphasis*] (Liang 2025, 1). The proliferation of drone-related technologies and ease of access via commercial suppliers such as FPV-drones are likely to further exacerbate this trend, and the gap is possibly to grow in favor of the attackers (i.e. terrorists). Furthermore, this worrying trend is likely to bring about

dual-use technologies challenges like the ones of nuclear proliferation, which may look less technologically advanced but with a growing global footprint and various risks of spillovers.

Second, the related growing countertrend is “the weaponization [of drones] by both state and violent non-state actors highlights the need for comprehensive regulatory frameworks and proper counter-unmanned aerial systems (C-UAS) defense mechanisms” (Rassler and Veilleux-Lepage 2025). This trend resembles the other side of the dual-use trend, where the burden now shifts considerably on states and international institutions with capabilities in security governance globally (i.e. UN) and regionally (i.e. NATO). Admittedly, these institutions are likely to bring a new set of capabilities as well as challenges such as regulation, consensus-building, and burden-sharing. Still, the importance of regulation of Lethal Autonomous Weapons Systems (LAWS) is likely to grow more critical, and “*the heightened focus on LAWS and AI* over the past year has given regulation advocates some optimism that political pressure for international treaties might increase. Despite differing global visions on governance, both the U.S. and China share a concern about preventing terrorists from acquiring autonomous weapons” [*italics added for emphasis*] (Schori-Liang 2025, 2).

Third, critical infrastructure is also vulnerable, and “hardening thousands of locations against attack would be financially restrictive, at best. Probable infrastructure targets include fuel or water storage facilities, gas pipelines, power distribution plants and food supply locations, many of which are minimally or completely unmanned” (Pledger 2021). Especially, recent attacks on critical energy infrastructure during the Ukraine war via unmanned air and sea systems have put forward the growing risk of such attacks to be emulated by terrorists against ports, ships, oilrigs, undersea cables, energy infrastructure, power-plants such as the recent attacks against The Zaporizhzhia Nuclear Power Plant (NPP) in southeastern Ukraine, which is the largest nuclear power plant in Europe. These threats to critical infrastructure (e.g. NPP, oil-rigs, ports, food/energy storage facilities, etc.) and public events such as concerts and political gatherings, where masses come together have the potential to be used to amplify the risks posed by terrorists’ use of aerial and naval drones.

Autonomous drones (USV: Unmanned Surface Vehicles) present a significant threat to naval fleets. For instance, “Ukraine has demonstrated this by repelling large-scale Russian mechanized attacks and crippling Russia's Black Sea Fleet. It will be more challenging to defend port infrastructure and ships in harbor – the targets are obvious and a weaker power” (Schori-Liang 2025, 2). such as terrorists, without a navy can pose a serious asymmetric threat. According to Chinese analysts, *USVs have five advantages in combat: effective concealment, low cost to manufacture and use, strong destructive ability, intelligent modes of control, and potential to operate autonomously* with diversified attack modes. USVs have greater explosive power than air strikes and can *harness wolf group tactics* for greater destructive power. [*italics added for*

emphasis] (Goldstein and Waechter 2023). This challenge brings Critical Infrastructure Protections (CIP) to a key level for the counterterrorism community, with this trend likely to be used increasingly by terrorists with potential risks for the targeting of CBRN-facilities (Chemical, Biological, Radiological, Nuclear).

Future Advancements and Impact on NATO Allies and Partners

For terrorists, the barrier to entry is lowering while the lethality is increasing due to several converging trends:

- *AI and Autonomy:* Emerging AI-assisted targeting allows drones to operate in “GPS-denied” environments. Future terrorists may use autonomous drones that don't require a constant pilot link, making them immune to traditional radio-frequency jamming.

- *Drone Swarms:* The ability to launch coordinated, simultaneous attacks by dozens of drones can overwhelm current air defense systems, which are often designed to track single, larger targets.

- *Additive Manufacturing (3D Printing):* As 3D printing becomes more advanced, groups can manufacture entire drone frames and specialized components locally, bypassing international sanctions and supply chain monitoring.

- *The "Ukraine Blueprint":* Lessons from the Russo-Ukrainian War—such as the use of First-Person View (FPV) drones for high-speed precision strikes—are being studied and emulated by extremist organizations globally.

Table-2: Challenges to NATO by Drones with Terrorists

Threat Category	**Impact on NATO Operations**
Asymmetric Vulnerability	Millions of dollars in NATO missile interceptors (like the Patriot) are being used to shoot down drones that cost only $500–$2,000, creating a massive economic imbalance.
Infrastructure Protection	NATO’s domestic critical infrastructure—power grids, oil refineries, and communication hubs—is increasingly vulnerable to small-scale, difficult-to-detect drone sabotage.

Threat Category	Impact on NATO Operations
Airspace Sovereignty	Recent "drone incursions" on NATO's Eastern Flank (e.g., in Poland and the Baltics) have exposed gaps in low-altitude radar coverage and forced the alliance to re-evaluate its "Operation Eastern Sentry" protocols.

For NATO, the proliferation of drones by terrorists poses the above three challenges illustrated in Table-2. In response to these threats, NATO has launched the LCI-X (Layered Counter UAS Initiative) as a 2026 Beacon Project. This initiative focuses on 90-day learning cycles to rapidly integrate new sensors and "soft-kill" (jamming) or "hard-kill" (kinetic) technologies to protect Allied territory.

Conclusions and Recommendations

It is difficult to be conclusive while threats and technologies continue to interact beyond our imagination. This challenge is akin to the one of a pilot trying to fix the engines during flight. Still, we can have some conclusions based on the current state of the art and about the looming threats beyond the horizon, which are likely to grow in terrorists' hands. Therefore, this section is the beginning rather that the end of this horizon scanning; the counterterrorism community must keep the pace and keep climbing the learning curve while putting hard-earned lessons in practice.

> Current and future advances [in drone-related technologies] and the rapid popularization of drones for average consumers and businesses has created a market that will continue to drive the technological improvement of drones for the foreseeable future. Improvements will extend to sizes, form factors, energy storage, techniques for propulsion, sensors and the ability to utilize and integrate advanced computer capabilities. Collectively, these improvements will increase the range, lifting capacity and overall capabilities of drones, *making them both more lethal and more difficult to counter*. [*italics added for emphasis*] (Pledger 2021)

These technological advancements are open for terrorist-exploitation. Combined with the recent drone-related innovations from the Russia-Ukraine War, it can be foreseen that the terror drone landscape is poised for another eruption akin to the 9/11 terrorist attacks that may come sooner than expected in part because of the growing availability of battle-hardened fighters and tactics from Ukraine to MENA. Therefore, "as the counterterrorism community looks forward and prepares for drone

related ‘outputs’ from the Ukraine war, it should be concerned not just about speed, range, and scale, but also about the *creative convergence of these [disruptive] technologies*.” [*italics added for emphasis*] (Rassler and Veilleux-Lepage 2025)

To mitigate these risks, “counterterrorism strategies must adapt to the changing landscape of warfare. Key measures include enhancing drone defense systems and investment in anti-drone technology, including jamming systems and counter-drone units that are essential to neutralize the growing threat of weaponized UAVs” (Schori-Liang 2025, 2). These necessary adjustments to technological developments put forward the need for multi-stakeholder reflection by the counterterrorism community, so that the lessons learned can be followed by well-timed and proactive *strategic adaptation*.

References

Farrow, Alexander, “Drone Warfare as a Military Instrument of Counterterrorism Strategy”, *Air & Space Power Journal*, 2016.

Goldstein, Lyle and Nathan Waechter, China’s Naval Strategists Dissect Ukraine’s USV Strike on Russia’s Black Sea Fleet Base, *The Diplomat*, 23 March 2023.

Pledger, Thomas, “The Role of Drones in Future Terrorist Attacks”, Land Warfare Paper 137, *The Association of the United States Army*, February 2021.

Rassler, Dan and Yannick Veilleux-Lepage, “On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism”, *CTC-Sentinel*, March 2025.

Rollins, John, “Armed Drones: Evolution as a Counterterrorism Tool”, *Congressional Research Service*, 7 November 2023.

Özgen, C. and S. Kurt. 2025.” PKK’s Drone Attacks within the Perspective of Learning Organization and Türkiye’s Counter Reaction. *Bulletin of” Carol I” National Defense University*, 14(2): 93-113.

Sadik, Giray, *Countering Terrorist Activities in the NATO Territory and Periphery*, Volume 10, Number 5, 2025. ISSN 2957-7160. Avalable at: www.openpublications.org.

Schori-Liang, Christina, “Emerging Threats: Will the Use of New Technologies in the Russia-Ukraine War Transform the Capabilities of Terrorists?” in Sadik, Giray (editor), *The Effects of the Russia-Ukraine War On Countering Terrorism*, NATO Centre of Excellence Defense Against Terrorism, Ankara, Türkiye, 2025. (1)

Schori-Liang, Christina, “Ten Lessons from the Russia-Ukraine War”, *Global Terrorism Index*, 2025. (2)

Yayboke, Erol and Christopher Reid, “Counterterrorism from the Sky? How to Think Over the Horizon about Drones”, *CSIS-Briefs*, May 2022.

CHAPTER 7

Terrorist Recruitment and Online Social Engineering: Technology, innovation and future global trends

Prof. Richard J. Aldrich

Abstract

"Move fast and break things" was an early Silicon Valley motto, now almost forgotten. But it might be taken as emblematic of our age in which the digital is still about speed and disruption. Digital has not only weakened state authority, but it has also subverted many of the intellectual categories and organisational boundaries in this realm, including the divide between different types of terrorist activity that we used to think of as discrete. In this essay we identify the wider tactical effects of technology on terrorist propaganda and recruitment including secondary cycles that connect other functions like communications and financing. We know less about extreme-right ideologies than religiously motivated violent extremism but globally, terrorists and extremists are starting to utilize these emerging technologies for recruitment, employing social media, the dark web and generative AI. While many attacks still use low-tech methods, technology is increasingly important for planning, preparation, and promotion. Actors use mobile payment systems, online exchanges and wallets, crowdfunding, peer-to-peer online fund transfers and the solicitation of donations on social media platforms. Overall, the most alarming aspect of terrorists embracing digital technology is cultural change, since it encourages new kinds of participants to innovate in a realm where, historically, change has been slow. We suggest creative terrorist groups are dangerous because of their potential to inflict surprise.

Introduction

The recent past is often a guide to the immediate future. The expert consensus is that social media and digital communications technologies have not only become key tools for terrorists and violent extremists, including white supremacists and religiously motivated extremists, to facilitate radicalization, recruitment, but also have also spread their violent ideas to other kinds of groups. In the last decade online forums and chat rooms, often with some encrypted protection, have replaced static websites as the main platforms for spreading violent extremist religious propaganda,

creating online networks, building communities and increasing confidence. Here, anonymity provided by encryption can foster stronger feelings of connection and coherence among individuals involved in extremist movements. In the future, gaming is also likely to be more important including interactive gameplay for promoting the strategic communication and propaganda aims of a group together with training (Robinson and Whitaker 2020).

In 2017, Maura Conway exhorted us to give more attention to terrorism and the internet and so scholars have now been busy for a decade. We argue that the more recent scholarship has moved beyond mono-causal “techsplanations”. The older literature tended to suggest that the internet had helped to cause “radicalization” - itself a rather problematic term (Heath-Kelly 2013). Instead, it is now clear that technology serves as a complex facilitator and catalyst for terrorist organizations, and that online and offline dynamics complement one another, reinforcing extremist views. Technology often acts to accelerate secondary effects, typically smoothing the financing of real-world operations. However, here we argue that we need to move away from the problematic distinctions of online and offline, since, in many regions, especially Europe, these binaries have declining utility (Meleagrou-Hitchens, Alexander, and Kaderbhai 2017). Unfortunately, some of the recent writers on cyberstrategy have tended conceptualize “cyberspace” as a different place with alternative rules, but when thinking about technology and terrorism it is more helpful to emphasise convergence of the digital and the real (Li et al 2022).

We begin with issues of recruitment. Over the last few years, notable analysts and scholars have tried to address this by making use of the new primary data afforded them by extremist use of social media. As terrorist use of the internet continues to develop in line with a shifting online media environment, the answers to these questions will become clearer as we will simply have much more data. Overall, we argue that digital communication technologies have not only become a key tool for violent groups to facilitate propagandization, recruitment, and the spread of their ideologies, but also to proliferate ideas of terrorism to other groups that might have been considered merely extremist, radical or “fringe”. As these boundaries erode, regulators are faced with new challenges.

Artificial intelligence (AI) is often spoke of as the new kid on the block. In fact, the intelligence and security agencies have been using this for “data washing” for decades (Moran, Christou, Burton 2023). More recently, the platforms have touted AI as a useful tool for moderation, countering violent extremism in the social media context. But the headlong rush to invest in competing AI models, has also resulted in what has been described as the “democratization” of AI and so far, its main effect in the infosphere has been to exacerbate radicalization and polarization. Everywhere across society, AI is scaling up disinformation, reinforcing existing societal biases and increasing speed. We know that information and communication technologies play a

crucial role in polarization, often amplifying extremist content and contributing to societal fragmentation (Burton 2023).

However, we currently have a legacy data problem. Since 9/11 much terrorism research has been focused on groups like al Qaeda and DAESH or their affiliates. This is hardly surprising as DAESH, with its promise of a “cyber caliphate,” was an alarming prospect, indeed the US spent $11 billion on operations against DAESH in just three years (Liang 2017). But since 2017 there has been a gradual realization that right wing terrorism and extremism have been neglected (Mølmen and Ravndal 2023). Right wing violence often sits in a liminal space between terrorism and extremism. Terrorism is often defined as violent actions intended to influence government or intimidate the public for political aims. Meanwhile extremism is characterized as opposition to fundamental values like democracy and the rule of law but is not a criminal offense in many countries. We need more research in this space, and we know even less about some of the more exotic species, such as anti-technology movements and ecofascism (Lubrano 2025).

1. Recruitment

Online recruitment has evolved through three distinct phases. The first phase began in 1984 with early bulletin board systems used by far-right extremists, with pioneers like white supremacists Louis Beam deploying technology to connect activists across North America. Religiously motivated terrorists, including Al-Qaeda, were somewhat behind, adopting this approach a decade later (Guse 2011). The second phase, which began in 2005 was characterised by the use of major social media platforms like Facebook, Twitter, and YouTube. Ideology became central to promotion, with organizations providing distant guidance rather than direct operational control. DAESH utilized social media to promote their cause even attracting Western recruits and encouraging them to travel to conflict zones. Latterly, it also seems to have encouraged faster transition from organized groups to networks and then lone-actor terrorism. More individuals acted independently, often using simpler methods such as vehicle ramming and knives, making terrorism more accessible (Kenyon & Binder 2023)

The third phase began perhaps in 2015 and might be thought of as the post-Snowden decade. More sensitized to surveillance, this period was defined by end-to-end encrypted apps and a blend of ideologies, where humour and memes play a significant role in promotion, and attackers often share manifestos and cite predecessors (Schmid et al 2025). This, in turn, led to a more complex landscape of extremism, visibly confirmed by the Capitol Hill events in January 2021 and a dawning realisation that comfortable old-world categories that had separated terrorism, radicalism, extremism and fringe no longer applied (Johnson 2021).

In recent years social media has transformed the landscape, making it more accessible and personalized. It can now act as a gateway for individuals seeking identity, community, and purpose among extremist groups. Recent research suggests that the COVID-19 pandemic accelerated exposure to extremist rhetoric, with many individuals encountering radical ideas for the first time during lockdowns. Part of this is about demographic shifts. Modern extremists are often younger males who feel adrift and unhappy, with many "radicalized" online. But the pattern is complex with QAnon (a far-right conspiracy movement originating in the United States) appealing particularly to women. Wellbeing issues are prevalent among extremists, with studies indicating that many convicted terrorists have had mental health difficulties or past problems with addiction even if these issues are not presently visible (Herrington 2022).

Some argue that we are now facing a new decade in which the medium is the message. This school argues that we will see a new "wave" characterized by technological advancements rather than specific ideologies, comparable to major historical events that sparked previous waves. Instead of a particular ideology we are now perhaps seeing a "salad bar" blend of ideologies and a decentralized approach to violence, making it difficult to predict future attacks. The emergence of a further phase of extremism may already be underway, influenced or even defined by new technologies (Ware 2023).

As we see a wider range of groups from different backgrounds emerge, we will encounter a more complex and innovative use of technology. Some of the more recent far-right attacks have been characterised not only by racist ideas and anti-migrant campaigns but also by anti-technology and ecologist ideas. A range of different groups on the far right have exhibited an interest in technology both as a target and as an enabler (Lubrano 2025). In 2025, the UK jailed three neo-Nazis for plotting terror attacks on mosques and synagogues, who were creating guns with 3D-printers and had only ever met online (Brown 2025).

Meanwhile, many right-wing revolutionary movements in Western democracies have shifted from armed resistance to metapolitics as a means of achieving societal change and this has been accelerated by social media. Since 1945 we have seen first "Vanguardism" that involved a hierarchical elite group leading the charge for revolutionary change. This was followed by the "Cell System" consisting of semi-autonomous cells operating independently to maintain security against state repression. Thereafter "Leaderless Resistance" promoted decentralized actions by individuals rather than organized groups. Metapolitics now emphasizes online cultural influence and ideological change as a precursor to hoped-for revolution. But this strategic shift towards the mainstream still contains a potential for future violent actions as some members remain dissatisfied with nonviolent approaches (Ravdnal 2023).

There have been numerous contenders for the so-called “fifth wave of terror”, building on Rapaport’s widely discussed “Four Waves” concept. Adherents of Rapoport contend that religious terrorism represents the fourth or most recent wave (Rapoport 2022). Kaplan has pointed to local movements that manifest intense ethnic, racial, or tribal mysticism with the Lord's Resistance Army in Uganda as a paradigmatic exemplar of fifth wave (Kaplan 2020). Others have asked if there is a distinct and connected wave of right-wing terror, with events in Norway and New Zealand as exemplars (Byman 2023, Hart 2023). Some have even argued that the far right has mobilized the security discourse surrounding the religious (fourth) wave as an existential threat to justify their ideological narratives, amplifying this using social media. In other words, if there is a right wing terroristic fifth wave, it may partly be a populist and social media echo of the fourth wave (Auger 2020, Collins 2021).

What are the precise functions enabled by such online activity? Mølmen and Ravndal (2023) argue that studies of right-wing extremist violence are scarce but nevertheless suggest six social media mechanisms relevant to online cultivation and action:

1. Compensation: seeking online identities to address offline vulnerabilities including personal crises such as mental health issues or social disconnection.

2. Isolation: socially alienated individuals turning to online communities for belonging increasing susceptibility to radical narratives.

3. Facilitation: the internet provides access to extremist content and facilitates communication among like-minded individuals.

4. Echoing: the internet increases extremist beliefs through interaction with similar viewpoints and lowers inhibitions against violence.

5. Acceleration: online shortens the timeframe, quickening the adoption of extremist beliefs and actions.

6. Triggering: online highlights specific events that encourage individuals to commit acts of violence.

2.Terrorist propaganda and generative AI

Terrorist organizations have consistently evolved in step with societal advancements, expanding their operational capabilities through technological innovation. Traditional propaganda and recruitment efforts confined to local communities have been left far behind, terrorists now utilize cyberspace to reach a global audience. Generative AI, cheap and ubiquitous, presents significant risks in this landscape. Malicious actors, including terrorists, are increasingly viewing AI as a tool

to amplify their communications using deepfake and large language models. Tech-savvy groups like DAESH are experimenting with AI-driven tools to enhance propaganda, recruitment, even operational security, and planning. It has also given them a dangerous taste for innovation, so we need to consider how terrorism could further exploit such technologies in the next decade.

Like drones, AI is among several dual-use technologies that have become "democratized" and highly accessible (Rickli and Liang 2024, 118). Arguably this has more to do with a desire to encourage market excitement and widespread adoption despite corporate rhetoric about egalitarianism (Koplin 2023). What we might call the "proliferation" of AI means the barrier for terrorist organizations to harness its capabilities diminishes daily. Open-source AI tools and conversational models like ChatGPT and Gemini can be exploited to generate convincing false narratives, to automate recruitment and propaganda efforts, and conduct social engineering schemes that manipulate vulnerable individuals at scale.

Unregulated and uncontrolled AI proliferation poses profound risks that necessitate comprehensive policy responses. The trend toward "democratization" means that even individuals without technical skills can access open-source AI tools for malicious uses, such as creating deepfakes or even conducting cyberattacks. Governments, academia, and private industry have discussed proposed frameworks that regulate AI but so far this goal has mostly proved elusive due to fears of stifling innovation. Moreover, liberal intergovernmentalism that might, in past decades, have created unified standards is increasingly in short supply. As yet we have little understanding of how terrorists will exploit AI's capabilities in areas like biotechnology. Overall, the convergence of AI and terrorism is imminent, meanwhile a coherent global effort to mitigate its risks is far away (Kaminski 2023).

The proliferation of AI-driven tools such as deepfakes and social engineering techniques presents sophisticated challenges, including the creation of disinformation campaigns, targeted propaganda, and the manipulation of public opinion (Houser 2025). But this is not just about propaganda. The increasing accessibility and "democratization" of artificial intelligence (AI) pose significant concerns in terms of operational capabilities. Even states are skirting international regulation on military targeting systems, so what are terrorist groups likely to do? AI analysis is likely to degrade secrecy around critical national infrastructure and major targets such as data centers. Advancements in AI-powered 3D printing threaten to lower the barriers to weapon acquisition, allowing terrorists to print firearms or parts of explosive devices and bypass traditional channels and security checks. The potential development of AI-created precursors to bioweapons is especially concerning. Autonomous systems, such as the self-driving vehicles, now present on the streets of San Francisco, present possible platforms for the delivery of explosives. Is every automated taxi a potential VBIED just waiting to be hired?

3. Terrorist Communication & Encryption

The recruitment landscape has been significantly changed by the impact of encryption technologies and their wider public availability. While public key encryption pioneers promoted these ideas as early as the 1980s, several recent events have changed the landscape (Jarvis 2020). First, the Snowden revelations during June 2013 were seen by some Big Techs as a threat to their business model and they responded by selling improved security. Apple is perhaps the best example of this (Ahlam 2020). Second, many entities including states, cities and companies responded to the saga by opting for stronger data sovereignty and data localization. Third, higher personal security is seen as a partial defence to online crimes and scams, typically the adoption of VPNs and more encryption of personal data (Fratini & Musiani (2025).

After 2013, secure communication applications such as Snapchat, Wickr and Telegram had boomed due to their provision of instantaneous end-to-end encrypted communications and the additional ability to auto delete data. Prior to a failed 2015 attack in Garland Texas, the suspect reportedly exchanged 109 encrypted messages with a known terrorist overseas before his attack, while in the much more deadly events Paris in the same year, the attackers allegedly used encrypted communications to plan their operation (Coleraine 2016, 1-7). In the San Bernardino case, the attackers utilized encrypted devices, which posed significant challenges for law enforcement, leading to costly efforts to access the information. Junaid Hussain, a British operative, effectively used encrypted messaging apps to communicate sensitive information (Kaplan 2015).

Encryption of chat rooms was an increasing matter of concern in the United States and Europe because DAESH had moved to a social media model that blended, recruitment, propaganda and direction. Potential adherents were exhorted to “Come or kill”, in other words ideally travel to caliphate, live a life of glory, participate in the final battle but if you can’t travel, kill where you are. In March 2016, the FBI claimed that DAESH had now successfully “crowd-sourced” its terrorism agenda by inspiring their adherents to conduct most of its attacks (Coleraine 2016, 4) with encryption used to protect many of these processes.

However, encryption can mean many things. Our most common experience is “End-to-End Encryption” – often a selling point on modern smart phones. Current messaging apps encrypt messages from sender to recipient, allegedly preventing even service providers from accessing content and can auto-delete. This means that providers can only share metadata with law enforcement, in other words, who called who from where and when, but not content. Faced with rising crime, including rising phone theft, some people use full device encryption which protects data on devices like smartphones and computers, making it difficult for unauthorized users to access

information even if the device is lost or stolen. For decades journalists, civil right campaigners, criminals and terrorists have used older tools like VPNs and Tor help users hide their internet activity, complicating efforts to trace communications (Chen at al 2024).

None of these privacy enhancement methods are foolproof, as demonstrated by past law enforcement successes. In the Netherlands the courts seem to have been as effective prosecuting those using encryption as those who do not (Hartel and van Wegberg 2023). In fact, it is not so much the privacy technology but more the growing security awareness and aversion to all things electronic that matters. Terrorists often employ various strategies to enhance security, such as using burner phones and self-destructing messages to eliminate incriminating evidence. But most importantly they are increasingly adopting self-denying ordinances and simply staying away from technology altogether when engaged in major criminal acts. Intelligence agencies are shifting focus from breaking encryption to hacking software and exploiting user mistakes, indicating a need for new strategies. Intelligence agencies have adapted by exploiting software vulnerabilities and user errors rather than attempting to break encryption directly, or else employing data that is less protected. Encryption can also impede bulk collection and the related use of AI. As encryption continues to evolve, so too must the strategies employed by law enforcement and intelligence agencies to address the challenges posed by secure communications in the context of terrorism (Graham 2016).

4. Financing and Donations

Historically, significant success in counter-terrorism has involved the exhortation “follow the money”. The focus of terrorist financing studies has typically been about "where does the money come from and what is it used for?" Despite the significant professional investigatory focus on the financing of terrorism it remains somewhat understudied in academic terms. But it has become evident in recent years that it is not a discrete area of activity. Most terrorist groups continually struggle to generate sufficient funding to maintain their capabilities and so propaganda and recruitment now overlap with support and donations, blurring our familiar analytical boundaries. Securing reliable financing to support objectives is important and so the issue of resource permeates even those groups that might be seen as proxies like Hezbollah. This is because independent income permits greater freedom of action.

Hezbollah and many similar groups have been especially active in leveraging online crowdfunding and cryptocurrencies. Some have argued that they display “sophisticated exploitation of digital finance for discreet resource accumulation, circumventing traditional oversight.” Crowdfunding in particular links funds more closely to recruitment propaganda and radicalization, and it also lowers the possible

risk for any donors, since the individual sums offered might be small and therefore unlikely to attract legal sanction (Farber & Yehezkel 2024).

Some organizations appear to have placed criminal activity at the centre of their financing models. This can also overlap with recruiting issues, since crime, typically credit card fraud or online scams, require particular skill sets. Much has been made of terrorist excursions into the trafficking of drugs and rare species as a source of income (Felbab-Brown 2018). Focusing on criminal activities has proved critical for terrorist financial survival when there have been undulations in donations, typically because of a loss of controlled territory. Kidnap-for-ransom has also been a perennial fund-raising tool for terrorist groups and this also requires the recruitment and retention of particular types of individuals. Thereafter, moving funds raised from third parties presents terrorist groups with considerable challenges and again requires specialist techniques (Shortland 2019). Terrorist groups reveal themselves to be primarily opportunistic and the need for money drives technical innovation and an increasing hunger for tech capable people (Keatinge & Danner 2021).

The global counter terrorist financing regime (CTF), now significant in scale, was primarily established in response to religiously motivated terrorism post-9/11, focusing on threats posed by groups misusing religious rhetoric. Global CTF efforts have largely neglected the rising trend of extreme right-wing terrorism in Europe and North America. Meanwhile, right-wing terrorism is often perpetrated by lone actors or small cells, leading to limited fundraising needs. Right-wing extremist groups primarily raise funds through events, merchandise sales, and donations. Donations are solicited through crowdfunding, wealthy donors, and discreet peer-to-peer transactions. Peer-to-peer transactions are common, with low-value donations aimed at preserving anonymity (Keatinge, Keen, and Izenman, 2019).

Partly for ideological reasons related to libertarianism, the right has been especially attracted to cryptocurrency. Terrorist funding methods can include state funding, legal businesses, and illegal activities such as drug trafficking and extortion, since all these benefits from discreet transfer and so since 2014, terrorist organizations have begun using cryptocurrency as an enabler. Terrorist organizations have utilized cryptocurrency for various illicit activities, including fundraising and transactions. Examples have even included the use of Bitcoin for ransom payments and funding operations, as seen in the 2016 Jakarta attacks. Recent reports indicate that terrorist networks and drug syndicates in or linked to India increasingly prefer Bitcoin for transactions (Akcinaroglu & Shi 2023).

Since 2024, the attractiveness of crypto currency for terrorist organisations has increased because of support by western governments and growing formal recognition from traditional markets. Anti-money laundering and counter-terrorism financing organisations worry that they cannot effectively prevent misuse of this expanding

landscape. Clear definitions and responsibilities for virtual asset service providers are necessary for better regulation. Legislative protection and international cooperation are essential to address the challenges posed by cryptocurrency. But this is not the current direction of travel and improved anonymity features in cryptocurrencies enhance their appeal for illicit activities and meanwhile we are seeing expansion of the cryptocurrency market and increased user acceptance (Wang and Zhu 2021).

5.The Big Techs

In previous decades terrorist organisations were primarily engaged in a contest with the state and some commentators still see governments as the principal guardians in the realm of counter terrorism (Cronin 2020). But when we think about recruitment and related issues, in fact major social media corporations like Meta (Facebook), Google, and X (Twitter) have become significant players in countering terrorism and violent extremism. Initially, the rise of DAESH prompted these companies to act beyond legal requirements due to reputational pressures and potential legislation. The firms have established a global governance regime for limiting terrorist communications. Indeed, the push back against DAESH propaganda involved not only states and corporations but also hacktivist groups like Anonymous, and these various actors were not always the most comfortable of bedfellows (McCrow-Young and Mortensen 2021).

Initially, platforms framed their role as mere conduits for information, distancing themselves from any responsibility for content. However, the alarming terror attacks between 2015 and 2017 led to increased pressure for self-regulation and proactive measures by platforms. Public and governmental scrutiny forced these companies to engage in counter-terrorism discussions and initiatives. There was a recognition that the relationship between terrorism and media has evolved, with social media becoming a primary tool for terrorist propaganda (Shehabat et al 2017).

Founded in 2017, the Global Internet Forum to Counter Terrorism (GIFCT) is a consortium of companies spearheaded by Meta, Google/YouTube, Microsoft and X. It stepped up as an operational organisation in 2019 and its membership quickly expanded to include 21 companies as of the end of 2023. GIFCT began as a shared hash database of DAESH-related material but expanded to include a wider array of violent extremist content in the wake of the attack on two mosques in Christchurch, New Zealand that was livestreamed on Facebook. GIFCT maintains a database of perceptual hashes of terrorism-related videos and images that is submitted by its members, and which other members can voluntarily use to block the same material on their platforms (Thorley and Saltman 2023).

Initiatives like the EU Internet Forum and the TERREG legislative proposal also emerged from this pressure. In Europe, social media companies now face not only

reputational risks but also potential financial losses if they fail to address terrorist content effectively. On 7 June 2022, Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online became applicable. This required internet companies in the EU to take swift measures to prevent the misuse of their services for dissemination of terrorist content. The new legal framework aims at preventing terrorists from easily exploiting the internet to recruit, encourage attacks, provide training and glorify their crimes. However, all this did not prevent the livestreaming of a further terrorist attack in Buffalo, USA in May 2022 (Wahl 2022).

Social media firms have developed self-regulated policies and technologies to combat terrorist content on their platforms. Companies have implemented extensive content moderation systems, including algorithmic moderation to detect and remove terrorist content. Facebook reported that 99.7% of terrorist content was detected before being flagged, while YouTube reported 98%. The shift from human flagging to automated systems using AI reflects a significant change in corporate governance and responsibility.

However social media companies now have to navigate the complex landscape of defining terrorism and terrorist content versus “extremism”. Governments often frame right-wing extremism as "hate crimes" rather than "terrorism." Meta has established a clear ban on terrorist organizations, while X and Google have been more ambiguous in their definitions. The reluctance to engage with the political aspects of terrorism and extremism reflects a desire to maintain an apolitical stance. This ambiguity can lead to challenges in effectively moderating content and addressing the nuances of terrorism.

Moreover, their algorithmic moderation tools were primarily designed to combat DAESH and al Qaeda propaganda. These tools are less effective against other forms of violent extremism, particularly far-right extremism, due to their fragmented nature. Platforms like YouTube trained their AI on over 2 million hand-reviewed DAESH videos, making the tools effectively non-transferable to other groups. Understandably, the tools focus on identifiable characteristics, such as logos, rather than the broader concept of "terrorism"- a notoriously tricky definitional and conceptual landscape (Borelli 2023).

Big Techs have notably uneven policies and diverse practices. In 2025, the controversial right-wing figure Tommy Robinson was charged by the UK government under counter-terrorism legislation and claimed that Elon Musk was paying for his defence (Quinn 2025). Potentially, this puts major governments who are trying to combat extremism on a direct collision course with some of the Big Techs. The very fact that global tech entrepreneurs might possibly lend support to this sort of figure is a wake-up call in terms of the issues around terrorist recruitment and extremist propaganda (Borelli 2023). Overall, this points us towards bigger problems. We used

to presume that states supported the rule based liberal international order and opposed terrorism and organised crime, but we have now been required to rethink that assumption (Felbab-Brown 2017). It is increasingly clear that the Big Techs are somewhat divided over violent extremism.

Moreover, when it comes to issues of web hosting for chat rooms or crowdfunding, the Big Techs do not own all the turf by any means. Smaller outfits have set themselves up in opposition to the larger entities, who they perceive to be politically biased and unjustly “censorious” toward conservative causes. The Alt-Right has conjured into existence a growing array of “Alt-Tech” companies pursuing a “second internet”, free from state interference and regulation (Donovan et al., 2019, Wade 2024). John Perry Barlow’s famous language of the “wild frontier” and claims to the independence of cyberspace are still alive and well in some corners of the internet.

Conclusion

Clearly, the future prospects for terrorism and extremism will involve the exploitation of emerging technologies like AI for propaganda and attack planning, the increased use of commercial drones and 3D-printed weapons, and the leveraging of the internet for recruitment, funding, and communication, with all these activities increasingly mixing. Government counter-terrorism agencies are fighting back by utilizing technology to enhance their own capabilities in surveillance, analysis and strengthening international cooperation. They have been actively joined by some elements of the private sector, with Meta forming a standout example.

Long-term, the most alarming threat that emerges as a consequence of terrorists embracing digital technology is cultural, simply because it encourages new kind of participants to innovate in a realm where, historically, change has been slow (Dolnik 2007). Some argue that this is now changing, and we are seeing an acceleration of terrorist innovation (Lampe et al 2024). Innovative terrorist groups are rather dangerous because of their potential to inflict strategic surprise upon states (Lubrano 2023). Moreover, the conventional categories and functional typologies that we used down the decades to analyze terrorist activity, including “recruitment” and “funding”, seem to be blurring and shifting. Digital innovation consistently disrupts familiar boundaries, eroding regulation and requiring us to rethink our strategies.

References

Ahlam, Rafita (2020) "Apple, the government, and you: Security and privacy implications of the global encryption debate." *Fordham Int'l LJ* 44/1: 771.

Amarasingam, Amarnath, and Marc-André Argentino (2020) "The QAnon conspiracy theory: A security threat in the making." *CTC Sentinel* 13/7: 37-44.

Akcinaroglu, S., & Shi, M. (2023) “Exploring the Impact of Cryptocurrency on Terrorism.” *Terrorism and Political Violence* 37/1: 111–135.

Auger, V. (2020) “Right-Wing Terror: A Fifth Global Wave?” *Perspectives on Terrorism* 14/3: 87–97.

Borelli, Marguerite (2023) “Social media corporations as actors of counter-terrorism.” *New media & society*, 25/11: 2877 –2897

Brown, Mark (2025) “Three neo-Nazis jailed for plotting terror attacks on UK mosques and synagogues.” Guardian, 17 October 2025.

https://www.theguardian.com/politics/2025/oct/17/three-uk-neo-nazis-jailed-for-between-eight-and-11-years-over-terror-plots

Burton, Joe (2023) "Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence." *Technology in Society* 75/1: 102262.

Burton, Joe (2023) "Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence." *Technology in society* 75/1: 102262.

Byman, Daniel. (2023) "Is there a wave of right-wing terrorism? A review article." *Political Science Quarterly* 138/2: 251-270.

Chen, Zhicong, et al. (2024) "Seeking anonymity on the Internet: The knowledge accumulation process and global usage of the Tor network." *New Media & Society* 26/2: 1074-1095.

Colraine, James (2016) “Encrypted Messaging Apps in the Age of Terrorism and Snowden: Savior or Safe Haven?” MA Dissertation, Georgetown University.

Collins, Jonathan (2021) "A new wave of terrorism? A comparative analysis of the rise of far-right terrorism." *Perspectives on Terrorism* 15/6: 2-22.

Conway, Maura (2017) “Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research.” *Studies in Conflict & Terrorism* 40/1: 77–98.

Cronin, Audrey K., (2020) *Power to the People: How Open Technological Innovation is Arming Tomorrow’s Terrorists.* Oxford: Oxford University Press.

Dolnik, Adam (2007). *Understanding terrorist innovation: Technology, tactics and global trends*. London: Routledge.

Dyntu, Valeriia, and Oleg Dykyj (2021) "Cryptocurrency as an instrument of terrorist financing." *Baltic journal of economic studies* 7/5: 67-72.

Farber, S., & Yehezkel, S. A. (2024) “Financial Extremism: The Dark Side of Crowdfunding and Terrorism.” *Terrorism and Political Violence* 37/5: 651–670.

Felbab-Brown, Vanda (2018) "Wildlife and drug trafficking, terrorism, and human security." *Prism* 7.4 (2018): 124-137.

Felbab-Brown, Vanda (2017) "Organized crime, illicit economies, civil violence & international order: more complex than you think." *Daedalus* 146/4: 98-111.

Fratini, Samuele, and Francesca Musiani. (2025) "Data localization as contested and narrated security in the age of digital sovereignty: The case of Switzerland." *Information, Communication & Society* 28/8: 1368-1386.

Ganor, Boaz (2021) "Artificial or human: A new era of counterterrorism intelligence?" *Studies in Conflict & Terrorism* 44/7: 605-624.

Graham, Robert (2016) "How terrorists use encryption." *CTC Sentinel* 9/6: 20-25.

Hart, Amber. (2023) "Right-wing waves: Applying the four waves theory to transnational and transhistorical right-wing threat trends." *Terrorism and Political Violence* 35/1: 1-16.

Hartel, Pieter, and Rolf van Wegberg (2023) "Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases." *Crime Science* 12/1: 5-12.

Heath-Kelly, Charlotte (2013) “Counter-terrorism and the counterfactual: Producing the ‘radicalisation’ discourse and the UK PREVENT strategy." *The British Journal of Politics and International Relations* 15/3: 394-415.

Herrington, Lewis, *Understanding Islamist Terrorism in Europe: Drugs, Jihad, and the Pursuit of Martyrdom.* London: Routledge 2022.

Holbrook, Donald. (2025) "Why They Fight: Ideology and Terrorist Motivation." *Terrorism and Political Violence* 37.7: 945-960.

Houser, Tyler & Beidi Dong (2025) “The Convergence of Artificial Intelligence and Terrorism: A Systematic Review of the Literature.” *Studies in Conflict & Terrorism*.

Jarvis, Craig (2020) *Crypto wars: the fight for privacy in the digital age: A political history of digital encryption*. New York: CRC Press.

Johnson, Bethan (2020) "Financing Right-Wing Extremism and Terrorism." *Research Briefing No. 5, Project CRAAFT*: 1-7.

Kaminski, Margot E. (2023) "Regulating the Risks of AI." *BUL Review* 103 (2023): 1347-1402.

Kaplan, Rebecca (2016) “Encrypted Messages: Does the Government Need a Way In?,” CBS News, November 16, 2015, http://www.cbsnews.com/news/paris-attacks-encryptedmessages-does-the-government-need-a-way-in/.

Keatinge, Tom, and Kerstin Danner (2021) "Assessing innovation in terrorist financing." *Studies in Conflict & Terrorism* 44/6: 455-472.

Keatinge, Tom, Florence Keen, and Kayla Izenman (2019) “Fundraising for Right-Wing Extremist Movements.” *Royal United Services Institute Journal* 162/2: 18-24.

Koplin, Julian J. (2023) "Dual-use implications of AI text generation." *Ethics and Information Technology* 25/2: 32-43.

Lampe, H., Herschinger, E., Nitzl, C., & Willems, J. (2024) Predicting Novel Terrorism: Media Coverage as Early-Warning System of Novelty in Terror Attacks. *Terrorism and Political Violence*, 37/5: 610–631.

Li, Kai, et al. (2022) "When internet of things meets metaverse: Convergence of physical and cyber worlds." *IEEE Internet of Things Journal* 10.5: 4148-4173.

Liang, Christina Schori (2017) "Unveiling the" united cyber caliphate" and the birth of the e-terrorist." *Georgetown Journal of International Affairs* 18/3: 11-20.

Lubrano, Mauro, (2023) “Navigating Terrorist Innovation: A Proposal for a Conceptual Framework on How Terrorists Innovate.” *Terrorism and Political Violence* 35/2: 248–63.

McCrow-Young, Ally, and Mette Mortensen (2021) "Countering spectacles of fear: Anonymous’ meme ‘war’against ISIS." *European Journal of Cultural Studies* 24/4: 832-849.

Meleagrou-Hitchens, Alexander, Audrey Alexander, and Nick Kaderbhai (2017) "The impact of digital communications technology on radicalization and recruitment." *International Affairs* 93/5: 1233-1249.

Mølmen, Guri Nordtorp & Jacob Aasland Ravndal (2023) “Mechanisms of online radicalisation: how the internet affects the radicalisation of extreme-right lone actor terrorists.” *Behavioural Sciences of Terrorism and Political Aggression* 15/4: 463-487.

Montasari, Reza (2024) *Cyberspace, cyberterrorism and the international security in the fourth industrial revolution: Threats, assessment and responses*. Cham: Springer International Publishing, 109-133.

Moran, Christopher R., Joe Burton, and George Christou (2023) "The US intelligence community, global security, and AI: From secret intelligence to smart spying." *Journal of Global Security Studies* 8/2: 1-18.

Pelzer, Robert (2018) “Policing of Terrorism Using Data from Social Media.” *European Journal for Security Research* 3: 163–79.

Quinn, Ben (2025) “Tommy Robinson says Elon Musk is paying his legal costs as trial begins.” *Guardian*, 13 October 2025. https://www.theguardian.com/uk-news/2025/oct/13/tommy-robinson-says-elon-musk-is-paying-his-legal-costs-as-trial-begins

Rapoport, David C. (2022) *Waves of global terrorism: From 1879 to the present*. New York: Columbia University Press.

Ravndal, Jacob Aasland (2023) "From bombs to books, and back again? Mapping strategies of right-wing revolutionary resistance." *Studies in Conflict & Terrorism* 46/11: 2120-2148.

Rickli, Jean-Marc, and Christina Liang (2024). "New and Emerging Technologies for Terrorists." In Max Abhams ed. *The Routledge Companion to Terrorism Studies*: 118-126. London: Routledge.

Robinson, Nick, and Joe Whittaker (2020) "Playing for hate? Extremism, terrorism, and videogames." *Studies in Conflict & Terrorism*: 1-36.

Schmid, Ursula Kristin, Heidi Schulze, and Antonia Drexel (2025) "Memes, humor, and the far right’s strategic mainstreaming." *Information, Communication & Society* 28/4: 537-556.

Shehabat, Ahmad, Teodor Mitew, and Yahia Alzoubi. (2017) "Encrypted jihad: Investigating the role of Telegram App in lone wolf attacks in the West." *Journal of strategic security* 10/3: 27-53.

Shortland, Anja (2019) *Kidnap: Inside the ransom business*. Oxford: Oxford University Press.

Thorley, T. G., and E. Saltman (2023) "GIFCT tech trials: Combining behavioural signals to surface terrorist and violent extremist content online." *Studies in Conflict & Terrorism*: 1-26.

Vashishtha, Nikita. (2023) "Artificial intelligence-assisted terrorism: A new era of conflict." 29 August 23 https://www.vifindia.org/article/2023/august/29/Artificial-Intelligence-assisted-Terrorism-A-New-Era-of-Conflict?slide=$slideshow$

Wade, Matthew, Stephanie A. Baker, and Michael J. Walsh. (2024) "Crowdfunding platforms as conduits for ideological struggle and extremism: On the need for greater regulation and digital constitutionalism." *Policy & Internet* 16/1: 149-172.

Wang, Shacheng, and Xixi Zhu (2021). "Evaluation of potential cryptocurrency development ability in terrorist financing." *Policing: A Journal of Policy and Practice* 15/4: 2329-2340.

Wahl, Thomas (2022) “Rules on Removing Terrorist Content Online Now Applicable.” EUCRIM 2/2022, p.112. https://eucrim.eu/news/rules-on-removing-terrorist-content-online-now-applicable/

Ware, Jacob (2023) "The third generation of online radicalization." *Program on Extremism at George Washington University*.

CHAPTER 8

Future Terrorism, Extremism, and the Rise of Single-Issue Ideologies: Strategic Lessons from Ontological Security

Dr. Lewis Herrington

Abstract

Future terrorism is likely to be shaped less by large, coherent ideological movements than by atomised extremism, single-issue causes and digitally accelerated radicalisation. This chapter argues that many emerging extremist movements, including right-wing extremism, far-left extremism, anti-state extremism and technology-related grievance movements, exploit a wider crisis of ontological security: the loss of belonging, agency and a coherent sense of meaning. As older sources of social stability have weakened, alienated individuals, especially younger citizens, may engage with radical causes less because of settled doctrine than because these causes offer identity, certainty and immediate purpose. Ontological insecurity does not cause terrorism directly. Rather, it can increase susceptibility to extremist narratives when combined with social isolation, perceived agency loss, identity fusion, sacred values and enabling digital environments. Digital platforms intensify this process by creating synthetic communities, reinforcing affective polarisation and elevating political demands into moral absolutes that resist compromise. These vulnerabilities also create opportunities for hostile states, which can exploit domestic polarisation through cognitive warfare, disinformation and reflexive control. The central lesson for counter-terrorism is that future resilience cannot depend only on policing, intelligence or disruption. Democratic states must also reduce the social and psychological conditions that make extremist narratives attractive. A National E-Education Strategy, combining critical reasoning, digital literacy and civic resilience, is proposed as a practical counter-terrorism measure to strengthen citizens against radicalisation, manipulation and future AI-enabled targeting.

1. Introduction

Contemporary politics is increasingly characterised by the fragmentation and proliferation of single-issue ideologies, some of which now contribute to extremism and terrorism. Such fragmentation represents a notable departure from the bipolar ideological clashes that defined much of the twentieth century and is likely to accelerate. For counter-terrorism practitioners, these developments matter because single-issue causes can provide a route into violent extremism, including right-wing

extremism, far-left extremism, anti-state extremism and technology-related grievance movements. Rather than treating these causes as isolated cultural disputes, they should be understood as potential pathways into terrorism when they fuse identity, grievance and a sense of existential threat. Although these movements differ in aim and language, many perform a similar psychological function by offering belonging, limits and meaning when mainstream society feels unstable or inaccessible. Questioning the tendency of modern political analysis to explain violent rebellion primarily through economic inequality, cultural polarisation or propaganda, this chapter argues that biological and psychological needs also help explain why ideological fragmentation can become attractive. When people lack belonging, acceptance, agency and narrative coherence, they lose ontological security. Insecurity of this kind does not cause terrorism directly. Rather, it can increase susceptibility to extremist narratives when combined with social isolation, perceived agency loss, identity fusion, sacred values and enabling digital environments.

Ontological security is an increasingly influential psycho-sociological concept in Security Studies describing a stable, continuous sense of self, order, and reality. Coined by psychoanalyst R.D. Laing and popularized by sociologist Anthony Giddens, it refers to "security of being"—the foundational confidence that the world and one's identity are stable and predictable (Mitzen 2006). Historically, ontological security was embedded in daily life through kinship, ritual, religion, community and shared moral order. Ancestral tribes and religious institutions provided belonging, limits and meaning, while later political and economic systems attempted to replace these older sources of stability. As those structures weakened, the search for meaning increasingly moved toward politics, identity and culture.

Within this context, “ideological tourists” may be attracted to extreme-left, extreme-right, anti-state or single-issue movements, sometimes moving between causes that are not logically consistent. Used analytically rather than dismissively, the term describes a form of transient ideological engagement in which individuals sample radical movements in search of identity, certainty, belonging and agency. Many such individuals do not initially engage with extremism because they fully understand or believe a settled doctrine. Instead, they are drawn to movements that offer an immediate community, a clear enemy, a simplified explanation of suffering and a role within a wider moral struggle. Crucially, this kind of engagement can lower the psychological barrier to more serious radicalisation, making the ideological tourist an important archetype for modern, decentralised extremism and terrorism.

A six-stage structure underpins the chapter’s argument; each linked to the future of terrorism and counter-terrorism. It begins by explaining the human need for ontological security and the psychological importance of social integration, agency and narrative coherence. The second stage examines the decline of older sources of meaning and the failure of later substitutes, including totalitarian political faiths and

liberal consumerism, to provide durable belonging and purpose. Third, attention turns to exclusion from mainstream politics and the rise of single-issue ideological tourism, especially among younger citizens facing economic insecurity, digital saturation and overlapping crises. Fourth, the chapter explores the mechanics of contemporary radicalisation, including crisis of agency, affective polarisation, identity fusion, sacred values and the crossing of kinetic thresholds into violence. Fifth, it considers how hostile states can exploit these vulnerabilities through cognitive warfare, disinformation, reflexive control and AI-enabled targeting. Finally, the chapter argues that future counter-terrorism requires a national resilience strategy grounded in E-education, critical reasoning, digital literacy and civic renewal. Its aim is not to pathologise dissent or collapse single-issue politics into terrorism. Democratic politics depends on protest, disagreement and focused campaigns. Danger arises when a cause becomes a total explanation for suffering, a substitute for belonging and a justification for violence against an existential enemy, often manifesting as terrorism.

2. The Human Need for Meaning

Ontological Security

Modern ideological instability is not only a political or philosophical problem. It is also a question of how people manage uncertainty, threat and belonging. Humans seek meaning, coherence and social attachment because these make the world more predictable, reduce psychological strain and help regulate fear. In political terms, this is closely related to ontological security, understood as the need for stable relationships, routines and narratives that make life feel intelligible and manageable (Giddens, 1991). When these supports weaken, individuals may become more vulnerable to ideologies that promise certainty, identity and purpose. For practitioners of counter-terrorism, the concept matters because it helps explain why citizens who feel socially adrift may become more open to extremist narratives. Radical movements do not only persuade through doctrine, they may also reassure by giving alienated individuals a community, a story and a restored sense of direction.

Three mutually reinforcing conditions are especially important as drivers. First, deep social integration provides the interpersonal foundation of ontological security. Drawing on Social Baseline Theory, Coan and Sbarra (2015) argue that the brain expects access to social relationships that mitigate risk and reduce effort. Trusted relationships allow individuals to share the burden of threat management, reducing the psychological cost of uncertainty. Where community, family, institutions and shared civic life erode, extremist movements may become attractive because they offer substitute communities with clear boundaries, shared enemies and a strong sense of collective identity. Second, flexible control helps individuals distinguish between stressors that can be changed and those that must be endured. McEwen (1998) describes allostatic load as the cumulative physiological wear and tear associated with

repeated or chronic stress. On this basis, an acceptance-based response to genuinely unavoidable hardship may reduce chronic arousal while preserving attention and effort for problems that remain open to agency. Politically, movements that promise total control over complex problems can offer psychological relief, even when their solutions are unrealistic, coercive or dangerous, even terroristic.

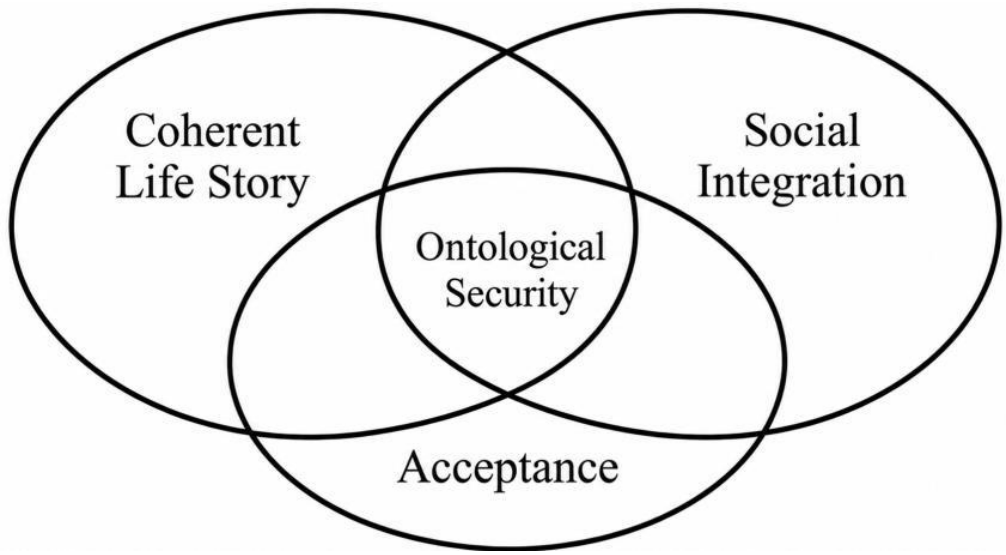


Figure 1 – Mutually Reinforcing Conditions that Contribute Towards Ontological Security

Existential narrative coherence forms the third condition. Friston's (2010) free-energy principle suggests that adaptive systems seek to minimise surprise to resist disorder and maintain viable states. A fragmented life story may therefore increase uncertainty, vigilance and the cognitive burden of interpreting events. By contrast, a coherent narrative offers a stable framework through which people can understand their place in the world. Ideological narratives can become powerful for this reason, even when they are simplistic. They reduce complexity, identify causes of suffering and give the individual a role within a larger story. Together, social integration, acceptance-based control and existential narrative coherence help underpin ontological security. They support belonging, the acceptance of unavoidable hardship and a durable sense of meaning and purpose. When mainstream institutions fail to provide these conditions, the search for ontological security can migrate toward more rigid and radical ideological systems. Such migration creates the psychological opening through which contemporary extremism and terrorism may gain traction.

Table 1 - Psychological Conditions that Support or Undermine Ontological Security

Psychological condition	Effect on ontological security	Cognitive or physiological mechanism	Likely behavioural outcome
Social isolation	Undermines belonging and increases perceived vulnerability	Absence of trusted relationships increases the individual burden of threat monitoring and emotional regulation	Anxiety, mistrust, withdrawal and susceptibility to substitute communities
Ambiguity and anomie	Undermines intelligibility and weakens the sense that life is manageable	Persistent uncertainty increases prediction error, cognitive strain and the search for simplified explanations	Attraction to rigid narratives that promise certainty, order and meaning
Loss of agency	Undermines the sense that action can shape outcomes	Repeated exposure to uncontrollable stressors increases allostatic load and can produce helplessness or chronic arousal (McEwen, 1998)	Resentment, fatalism or attraction to movements promising restored control
Deep social integration	Supports belonging and reduces perceived threat	Trusted relationships distribute the burden of risk management and reduce individual effort (Coan and Sbarra, 2015)	Resilience, trust, cooperation and lower vulnerability to extremist recruitment
Acceptance-based control	Supports stability by distinguishing changeable problems from unavoidable hardship	Flexible appraisal reduces futile effort directed at immutable stressors and preserves agency for solvable problems	Greater emotional regulation, endurance and reduced attraction to totalising solutions
Existential narrative coherence	Supports meaning by giving the individual a stable place within a wider story	Coherent narratives reduce uncertainty and provide a more stable predictive framework for interpreting events (Friston, 2010)	Purpose, continuity and reduced vulnerability to simplistic ideological explanations
Sacred values	Can provide synthetic certainty but may undermine democratic flexibility	Deontological reasoning elevates certain beliefs beyond compromise, negotiation or material trade-off (Tetlock, 2003)	Moral rigidity, out-group hostility and increased risk of extremist or terrorist violence

The Ancestral Scaffold of Belief

Human beings evolved in small groups where belonging was essential for survival. Social isolation in that setting was not simply unpleasant - it often proved fatal. Deep communal bonding therefore became a basic condition of human security, allowing individuals to share the burden of threat detection, distribute practical risk and reduce uncertainty. Early belief systems also helped make the world intelligible. Animism, for example, allowed early humans to understand the natural world as a community of responsive agents rather than as a series of random and threatening events. Bird-David (1999) argues that animist societies often treated animals, plants and natural forces as relational beings. Such beliefs gave people a framework for interpreting danger, misfortune and uncertainty. In modern terms, they supported ontological security by offering belonging, limits and a coherent story about humanity's place in the world.

Relevance for extremism and terrorism lies in the continuity of the underlying need. People still seek belonging, agency and meaning, even though the institutions available to meet those needs have changed. Contemporary citizens no longer inhabit small kinship groups in which social position, moral expectations and cosmological meaning are largely inherited. Instead, many must construct identity and purpose across fragmented social, digital and political environments. Where durable sources of ontological security weaken, individuals may become more receptive to radical ideologies that offer simple explanations, strong group identity and a clear account of blame. The persistence of ancestral belief systems therefore matter here not because modern extremism is primitive, but because they reveal the depth of the human need for ontological security that extremist movements continue to exploit. The problem is not that people seek meaning. It is that destructive movements such as terrorist organizations can provide synthetic forms of meaning when healthier sources of belonging and agency have failed.

How Religion Provided Stability

As early societies grew beyond small kinship groups, face-to-face bonds could no longer provide the same automatic level of social trust. Dunbar (1992) suggests that there are cognitive limits to the number of stable social relationships individuals can maintain. Once societies exceeded these limits, larger institutions were needed to hold communities together. Religion performed this function for much of human history. Rituals, morality and common accounts of suffering gave people a durable framework for belonging and interpretation. Worship, obligation and tradition connected individuals to communities that extended beyond immediate family. Religious narratives also gave hardship a place within a wider moral and spiritual order, allowing suffering to be interpreted through duty, discipline, sacrifice or redemption. In this sense, religion became one of the main historical sources of ontological security.

Stability of this kind also carried political risks. When religious institutions claimed exclusive access to truth, they could produce rigid boundaries between insiders and outsiders. Beliefs that gave one community coherence could invalidate another, especially when fused with state power, territory or collective identity. Over time, this helped fuel sectarian conflict and political violence. Such an observation does not imply that religion inevitably causes violence. Rather, it shows that powerful systems of meaning can stabilise communities internally while sharpening hostility toward those outside the group. A similar pattern remains visible in some modern forms of extremism and terrorism. Movements organised around nation, race, grievance, revolution, faith or single-issue causes can provide internal solidarity while constructing opponents as existential enemies. Religion therefore illustrates a wider principle. Systems that meet the human need for belonging and meaning can become politically dangerous when they close down uncertainty, sacralise boundaries and define compromise as betrayal.

Enlightenment and the Loss of Religious Scaffolding

In Europe, separation of church and state constituted a major achievement of the Enlightenment period. It reduced the direct role of religion in government and helped limit the political violence associated with sectarian rule. Yet secularisation also created a new problem. Religious institutions had not only exercised political power. They had supplied many people with identity, routine, belonging and meaning. Classical liberalism, associated with thinkers such as Locke (1689/1983), placed greater emphasis on individual freedom and private conscience. Such freedom was politically liberating, but it also shifted responsibility for meaning onto the individual. Citizens were increasingly expected to construct their own system of purpose, values and identity rather than inherit them from a stable religious order.

Narrative identity is psychologically demanding because individuals must connect memory, present experience and future aspiration into a coherent account of the self. Without shared external frameworks, that task can become more fragile. Liberalism therefore solved one problem while creating another. It reduced religious domination, but it did not fully replace the social and psychological functions that religion had performed. No immediate collapse followed. Instead, shared sources of ontological security gradually thinned. For many citizens, this produced uncertainty, restlessness or a more individualised search for meaning. Among those already alienated from mainstream institutions, however, the loss of inherited scaffolding created a vulnerability that extremist movements could exploit. Radical ideologies can relieve the burden of self-definition by providing a ready-made identity, a moral vocabulary and a clear account of where the individual belongs.

Infinite Aspiration and the Burden of Self-Definition

Modern liberal societies often encourage individuals to see themselves as the authors of their own destiny. Such a vision can be empowering, but it can also become burdensome. When people are told that identity, status and meaning are matters of personal choice, failure can feel entirely personal. Individuals are left to carry responsibilities that were previously shared by family, community, religion or class. Famously, Putnam (2000) documents the decline of voluntary associations and civic participation, suggesting that many of the networks that once supported social trust have weakened. These networks mattered because they allowed people to share problems, regulate anxiety and feel embedded in something larger than the self. As such bonds decline, the search for meaning becomes more individualised and more fragile. Durkheim (1897/1951) described this condition as “anomie,” in which social norms no longer provide effective limits or guidance. Without such limits, desire can become endless and people may experience chronic dissatisfaction. Frankl (1946/1984) later argued that the loss of meaning could contribute to aggression, depression and addiction. More recently, Case and Deaton (2020) have linked rising deaths of despair to wider patterns of social and economic breakdown.

For counter-terrorism, the lesson is direct. Extremism does not grow only from poverty, ideology or propaganda. It can also emerge from a deeper crisis of ontological security. Where people lack belonging, limits and a coherent story about their place in the world, radical movements can offer substitutes. Right-wing extremism, far-left extremism, anti-state extremism and single-issue ideologies may all provide the same basic psychological reward. Each can give the alienated individual a community, an enemy, a mission and a sense of restored agency. None of this means that insecurity automatically produces terrorism. Most insecure or alienated people never become violent. Nevertheless, democratic states should treat ontological insecurity as part of the wider threat environment. If mainstream institutions cannot provide credible forms of belonging, agency and meaning, extremist movements will continue to compete for that role.

3. Dissolution of Grand Narratives

Totalitarian Imitations of Religion

Following the rapid pluralisation of belief after the Enlightenment, new political systems emerged to supply the certainty once offered by religion. Fascist and communist regimes should therefore be understood not only as attempts to seize state power, but also as attempts to repair a crisis of ontological security. They offered large, simple stories about history, identity and destiny. Fascism promised national rebirth through discipline, hierarchy and loyalty to the leader. Communism promised class redemption through the supposedly scientific inevitability of proletarian revolution. In

both cases, politics took on a quasi-religious function by giving individuals a place within a wider historical mission. Leadership cults such as the *Führerprinzip* also restored an external locus of control. By surrendering judgement to the leader or party, the individual was relieved of some of the burden of self-definition. Totalitarian systems therefore supplied belonging, certainty and purpose, but only by demanding obedience and narrowing reality. That pattern remains important for understanding extremism today, since radical movements often become attractive when they appear to offer ontological security that mainstream institutions no longer provide.

Despite their capacity to mobilise mass support, totalitarian systems suffered from two basic weaknesses. First, they tried to manufacture social integration through coercion rather than trust. Genuine belonging depends on reciprocity, shared confidence and stable social bonds. Totalitarianism substituted these with surveillance, fear and forced conformity. Outward unity could be produced, but the system also increased the insecurity it claimed to resolve. Second, such regimes had to suppress empirical reality whenever it threatened the official story. Unlike older religious frameworks, which often operated through inherited ritual and tradition, totalitarian ideologies required continuous propaganda, censorship and policing. Considerable state energy had to be spent maintaining the fiction that the party, leader or doctrine could not be wrong. As a result, totalitarianism produced a brittle form of ontological security. It could organise loyalty and sacrifice in the short term, but it generated paranoia, distrust and resentment over time.

State communism's collapse between 1989 and 1991 revealed these limits clearly. Harrison (2001) argues that by suppressing market institutions and corrective feedback, the Soviet system produced technological stagnation and persistent shortages. The promise of collective security therefore failed at the material level as well as the psychological one. After transition, Wike et al. (2019) found that many citizens approved of democracy and market reform but also believed that the benefits had flowed disproportionately to elites. Mishler and Rose (2001) similarly identify institutional distrust as a central challenge for post-communist democracies. Totalitarianism failed because coercion and dishonesty could not provide durable ontological security. It could imitate religion by offering belonging, certainty and sacred political purpose, but it could not sustain the trust and coherence required for stable social life. For the study of terrorism and extremism, the lesson is that simplified political faiths can mobilise alienated populations, but their reliance on enemies, obedience and myth makes them prone to repression, radicalisation and violence.

False Promise of Liberal Consumerism

Where totalitarian regimes tried to impose meaning through the state, Western democracies increasingly looked to the market. Liberal consumerism promised a softer route to ontological security. It did not demand formal obedience to a party,

leader or doctrine. Instead, it suggested that individuals could build identity, purpose and agency through work, lifestyle, consumption and personal choice. For a time, this appeared powerful. During the Cold War, consumer capitalism offered a visible alternative to the shortages and coercion of state socialism. After the collapse of the Soviet Union, this model seemed to have won the ideological argument. Fukuyama (1992) famously described this moment as the “end of history”, in which liberal democracy and market capitalism appeared to represent the final form of political development. Yet this apparent victory concealed a deeper weakness. Consumerism could offer comfort, distraction and status, but it could not reliably provide the deeper foundations of ontological security.

Consumption produces only temporary reassurance. Buying goods, improving status or pursuing lifestyle goals may create short-term satisfaction, but these activities do not necessarily provide durable meaning, belonging or agency. Ryan and Deci (2001) argue that well-being depends on deeper psychological needs, including autonomy, competence and relatedness. A society organised mainly around consumption may stimulate desire without satisfying these needs. It encourages people to keep searching for identity through external acquisition, while leaving the underlying need for belonging and purpose unresolved. Consumerism also weakens social integration. Bauman (2007) argues that late modern consumer societies increasingly treat relationships as flexible, temporary and transactional. This matters because ontological security depends on stable social bonds. When neighbours, colleagues and fellow citizens are experienced less as sources of mutual support and more as competitors for status, housing, jobs or recognition, the social world becomes more threatening. Individual freedom then coexists with a more fragile form of selfhood, because each person is left to manage uncertainty with fewer durable forms of collective support.

This has direct relevance for extremism and terrorism. When mainstream society offers identity mainly through consumption, those who cannot access its rewards may feel humiliated or excluded. Even those who do access them may still experience emptiness, loneliness or status anxiety. Extremist movements can exploit this gap by offering what consumer society often cannot provide, including a strong community, a clear enemy, a sense of moral purpose and the feeling that personal sacrifice matters. Such dynamics help explain why radicalisation is not limited to the materially poor. It can also attract people who are socially isolated, spiritually restless or unable to locate themselves within a meaningful collective story.

Right-wing extremism is especially able to exploit the failures of consumer individualism. It can present liberal society as weak, rootless and decadent, while offering the promise of restored identity through nation, race, tradition or masculinity. Far-left and anti-capitalist extremism can exploit the same crisis from a different direction, presenting market society as corrupt, dehumanising and structurally violent.

Single-issue extremist movements may also gain traction by offering clarity in place of consumer confusion. Technology-related grievance movements can perform a similar function when they portray technological change, artificial intelligence or digital capitalism as the single cause of social dispossession. In each case, the appeal lies not only in the stated ideology, but in the psychological function it performs. Diffuse dissatisfaction is turned into a mission. The market therefore failed as a substitute religion. It could coordinate production, expand choice and create prosperity, but it could not carry the full weight of meaning. Individuals were asked to become entrepreneurs of the self while the communities and institutions that once helped people manage uncertainty continued to weaken. As McEwen (1998) suggests, chronic stress carries physiological costs. A society that continually intensifies competition, comparison and insecurity risks increasing that burden.

Neoliberal Acceleration of Agency Erosion

Latent weaknesses within liberal consumerism were intensified by the neoliberal turn that shaped Western politics from the 1980s and became dominant after the end of the Cold War. During the Cold War, Western states had strong reasons to protect the social contract. Welfare systems, labour rights and public services helped demonstrate that liberal democracy could provide security without authoritarian control. After the collapse of the Soviet Union, that external pressure weakened and the market increasingly became the organising principle of political life. This mattered for ontological security because citizens were encouraged to understand insecurity as a personal challenge rather than a shared political problem. Work, housing, welfare and community were exposed more directly to market forces, while individuals were told to adapt, compete and take responsibility for outcomes they often could not control. Government did not disappear, but it retreated from its role as a guarantor of stability, reassurance and collective protection behind the cloak of New Public Management. A widening gap then opened between the promise of personal freedom and the lived experience of lost agency.

Consequences for both politics and security followed. Berman and Snegovaya (2019) argue that centre-left parties across Europe moved toward the market-friendly centre, reducing the programmatic differences between mainstream political options. For many voters, this made democratic politics feel closed. If elections no longer appeared to offer a serious choice over the direction of economic life, mainstream democracy could seem less capable of delivering change. Economic restructuring reinforced this sense of lost agency. Stansbury and Summers (2020) identify a structural decline in worker power, reflected in stagnant wages and a falling labour share of income. Autor et al. (2021) show how import competition associated with the “China shock” accelerated deindustrialisation in many communities. These changes not only reduced income, but also damaged identity, status and the link between effort and reward. In places where work had provided social pride, local solidarity and a

sense of collective purpose, economic decline became a crisis of meaning as well as material security.

Neoliberalism promised that markets would increase prosperity, expand choice and reward effort. In practice, the benefits were unevenly distributed. Konczal et al. (2020) argue that the system generated higher inequality rather than broad-based economic security. For those who felt left behind, consumer capitalism became a visible reminder of exclusion. People were told they were free to succeed, but many experienced the conditions of success as increasingly unreachable. Resentment, humiliation, distrust and anger could grow from the gap between promise and experience. Right-wing extremism may redirect this toward migrants, minorities, “globalists”, liberal elites or other alleged internal enemies. Far-left extremism may frame the market order itself as a system of violence and exploitation. Anti-state and single-issue movements may present democratic institutions as captured, corrupt or incapable of reform. Across these movements, the attraction lies in the restoration of agency, identity, belonging and moral clarity. Erosion of agency under neoliberalism therefore created conditions in which some citizens became more susceptible to extremist or terrorist narratives promising restoration, revenge or total transformation.

Financial Rupture and The Decline of Trust

The global financial crisis of 2008 marked a decisive break in the belief that markets could reliably provide stability, opportunity and ontological security. Earlier downturns could be understood as temporary disruptions within a broadly functioning system, but the crash exposed a deeper failure in the moral logic of liberal consumerism. For decades, citizens had been encouraged to believe that effort, prudence and playing by the rules would produce security. Financial collapse reversed this expectation. State intervention protected major financial institutions, while many ordinary citizens experienced unemployment, austerity, wage stagnation and insecurity. Crawford (2015) describes this as a moral hazard problem, while Bresser-Pereira (2010) argues that the crisis exposed the limits of self-regulating markets rather than a merely technical failure. Its political effect was corrosive because the link between agency and outcome appeared to break. Individuals were still expected to manage risk personally, but the largest failures of risk were socialised by the state. Trust weakened not only in markets, but also in the political institutions that had defended them.

Aftermath of the 2008 financial crisis deepened this loss of confidence. Prolonged austerity, weak growth and rising inequality created fertile ground for populism, extremism and anti-system politics. Melios (2020) links declining political trust in Europe to corruption, economic discontent and the perception that political systems are unresponsive. OECD data suggests that, by 2024, only 39 per cent of people across member countries reported trust in their national government (OECD,

2024). Wider trust data points in the same direction. The Edelman Trust Barometer identifies government as one of the least trusted institutions globally (2024), while Pew Research Centre (2024) records broad dissatisfaction with the functioning of democracy in advanced economies. Distrust has also extended beyond government. The Reuters Institute's Digital News Report shows growing scepticism toward mainstream media, financial institutions and expert authority (Newman et al., 2024). This matters because ontological security depends partly on the belief that public institutions are legible, fair and capable of protecting citizens from intolerable instability. Once that belief collapses, extremist narratives and terrorists find a more receptive audience.

The United States illustrates the remarkable depth of this institutional rupture. The Pew Research Centre (2024) reports that only 20 per cent of American adults say they trust the federal government to do what is right, compared with 77 per cent in 1964. Such decline is not evenly distributed. Trust is especially low among groups that experience the social contract as historically unequal or broken, with the Pew Research Centre (2024) reporting lower levels of federal trust among Black and Hispanic Americans than among White Americans. A wider pattern is therefore visible. Many citizens now feel deprived of both older religious sources of meaning and the economic security once promised by consumer capitalism. In this vacuum, the search for ontological security moves increasingly into politics. Mainstream parties, however, are often perceived as technocratic, insulated and unable to provide meaningful agency. This creates an opening for right-wing extremism, far-left extremism, anti-state movements and single-issue ideologies, all of which can transform distrust into a clear story of betrayal, blame and restored control. Failure by markets and institutions to provide durable security has therefore created a population more susceptible to extremist narratives promising certainty, belonging and revenge.

Table 2 - Changing Sources of Ontological Security

Historical form	Social integration	Agency and acceptance	Existential narrative coherence
Ancestral tribes	Belonging was embedded in kinship, shared labour and direct communal survival.	Human limits were accepted through dependence on nature, ritual and group norms.	Animist belief systems made the natural world intelligible by treating it as relational and responsive.

Institutional religion	Regular worship, ritual and parish life created durable forms of community.	Suffering and limitation were interpreted through religious duty, discipline and acceptance.	Theology provided a shared story of human purpose, moral order and the individual's place in the world.
Totalitarianism	Belonging was manufactured through party loyalty, surveillance and enforced conformity.	Personal agency was surrendered to the leader, party or revolutionary project.	State myths of national rebirth or historical inevitability supplied a simplified political faith.
Liberal consumerism	Social bonds were weakened by competition, status anxiety and transactional relationships.	Choice was presented as freedom, but many individuals experienced insecurity as personal failure.	Meaning became privatised, with individuals expected to construct identity and purpose for themselves.
Single-issue ideologies	Online tribes and activist communities offer substitute belonging and strong group identity.	Disruption or violence can provide a synthetic sense of agency where formal politics feels closed.	Complex problems are reduced to simple moral binaries, giving the individual a clear enemy and mission.

4. Exclusion from Mainstream Politics

Gatekeeping and Limited Political Access

Left- and right-wing extremism are both strengthened when citizens conclude that ordinary political channels can no longer deliver meaningful change. Such exclusion is not only a civic grievance. It can also become a threat to ontological security because it weakens the individual's belief that action has consequences. Mainstream political parties once acted as important pressure valves, translating public frustration into representation, negotiation and policy reform. In the contemporary period, however, many voters experience these institutions less as vehicles for participation than as gatekeepers protecting established interests. Candidate selection, party discipline and internal control over policy agendas can limit the entry of new ideas into formal politics. Fiva et al. (2024) describe this as a gatekeeper's dilemma, in which parties must balance openness against control. When

that balance appears rigged in favour of insiders, the wider electorate may conclude that the system is insulated from public will. Such perceptions do not automatically produce extremism or terrorism, but they do create a psychological opening for movements that promise to bypass a blocked political order.

Once institutional routes appear closed, extra-parliamentary action can begin to look like the only remaining source of agency. Protest, disruption and civil disobedience, even terrorism, may then be interpreted not as irrational behaviour, but as attempts to regain bargaining power outside a system perceived as inaccessible. Walgrave et al. (2022) show that disruptive action is often used strategically to attract media attention and force issues onto the agenda. Hayes et al. (2024) make a similar point in relation to Extinction Rebellion, whose activists frame civil disobedience as necessary in the face of institutional failure. France's Gilets Jaunes movement also illustrates this dynamic. Royall (2019) links the movement to deep distrust of traditional parties, while Carpenter and Perrier (2023) show how blockage and occupation were used to make ignored grievances visible. These examples should not be collapsed into terrorism. Their relevance lies in showing how perceived exclusion can move political behaviour away from routine participation and toward more confrontational forms of action.

Brexit provides a different example of how institutional blockage can be challenged through the ballot box rather than through street-level disruption. Campaigners used simple moral claims about sovereignty, control and representation to mobilise voters who felt ignored by established parties and media institutions. Cox and Shapiro (2025) argue that single-issue referendums can unbundle complex policy questions, allowing highly motivated groups to exert disproportionate influence. This dynamic matters because it shows how single-issue politics can become a vehicle for agency when normal party competition appears ineffective. Other structural barriers may reinforce the same perception. Electoral systems can disadvantage minority interests (Rickard, 2017), while opaque political financing can strengthen the belief that influence is purchased rather than earned through democratic participation (Jakobsen, 2024). Where citizens believe that formal politics is closed, the search for ontological security may migrate toward radical movements that offer belonging, certainty and restored control. Political gatekeeping can therefore indirectly increase susceptibility to extremist narratives, including those associated with right-wing extremism and future terrorism.

Polycrisis Amidst Generation Z

Extremism is also shaped by the fragmentation of the neoliberal consensus amid the volatile environment inherited by younger citizens. Generation Z has entered political life at a moment when digital saturation, economic insecurity and global crisis have converged. Turner (2015) identifies this cohort as distinctive because its social

and political formation has occurred inside digital environments, where threat, comparison and grievance are constantly visible. Tooze (2018) describes the contemporary landscape as a polycrisis, in which different forms of instability overlap and amplify one another rather than appearing in sequence. For younger people, climate change, technological disruption, war, housing insecurity and economic precarity are not abstract future possibilities. They form the background conditions of adulthood. Hickman et al. (2021) found that climate anxiety impairs daily functioning for a significant proportion of young people, while Gallup and the Walton Family Foundation (2025) report substantial concern among Generation Z about the uncontrolled development of artificial intelligence. High-intensity war in Europe and continuing violence in the Middle East have further weakened the assumption that liberal democracies are moving toward greater peace and stability. In ontological security terms, this generation faces a world that can appear unstable, hostile and difficult to interpret.

Immediate material pressures intensify these wider shocks. Starostin (2025) reports that rising prices have become a primary political concern for young Europeans, while housing shortages continue to obstruct traditional pathways into adulthood. Lennartz et al. (2015) show how access to housing has become increasingly difficult for younger cohorts, and Arundel and Hochstenbach (2021) link this to delayed independence and prolonged reliance on family support. Such conditions matter because they weaken the ordinary markers through which people build agency, identity and a coherent life story. Secure housing, stable work and a plausible future have historically helped individuals locate themselves within society. When these become inaccessible, ontological insecurity deepens. External reality becomes harder to predict, while the need for internal order becomes more urgent. Research by Adam-Troian et al. (2021) is useful here because it links crisis conditions to threat-regulation processes through which individuals may seek stability, certainty and restored agency. None of this means that Generation Z is inherently extremist, nor that insecurity automatically produces terrorism. Most young people respond to instability without violence. Nevertheless, the combination of digital immersion, economic blockage and existential threat creates a population more susceptible to radical movements that offer certainty, belonging and restored agency. Right-wing extremism, far-left extremism, anti-state extremism, technology-related grievance movements and other single-issue ideologies can all exploit this search for ontological security by converting diffuse anxiety into a clear enemy, a simple story and a violent mission.

Single-Issue Ideological Tourism

Convergence between political exclusion, material insecurity and existential anxiety has created the conditions for a more fluid form of ideological engagement. Far-left ideological tourism has often been discussed in relation to Western activists

transferring loyalty to revolutionary causes abroad, but far-right ideological tourism is now equally important. In both cases, the individual may move toward radical politics less through settled doctrinal commitment than through the search for ontological security. When mainstream politics appears closed and everyday life feels unstable, single-issue ideologies can provide immediate belonging, certainty and agency. They offer a simplified explanation of what has gone wrong, identify a clear enemy and give the individual a role within a wider struggle. This helps explain why contemporary extremism often appears fragmented and unstable. The ideological tourist is not always committed to a complete political programme. Instead, they may attach themselves to causes that provide psychological relief, whether those causes concern climate, race, gender, immigration, technology, national identity or anti-state grievance. Used analytically rather than dismissively, the term describes transient movement between causes in search of identity, certainty and agency. In this sense, single-issue extremism functions as a substitute belief system for people who feel that older sources of meaning have collapsed.

Digital platforms intensify this pattern because they make political identity immediately available, emotionally rewarding and socially reinforced. Starostin (2025) identifies social media as a primary channel of political engagement for younger cohorts, and this matters because online spaces allow users to encounter ideology first as aesthetic, mood and community before they encounter it as doctrine. The attraction is often not intellectual rigour but emotional clarity. A radical movement can offer a ready-made community, a moral vocabulary and a sense of personal significance. This also explains why some individuals appear able to move between far-left, far-right, anti-state, conspiratorial and technology-related positions with surprising ease. One cause may condemn capitalism, another immigration, another artificial intelligence, another the state, yet each can perform the same psychological function. Specific content changes, but the underlying reward remains similar. Each ideology offers a way to reduce uncertainty, restore agency and place private distress within a larger public story.

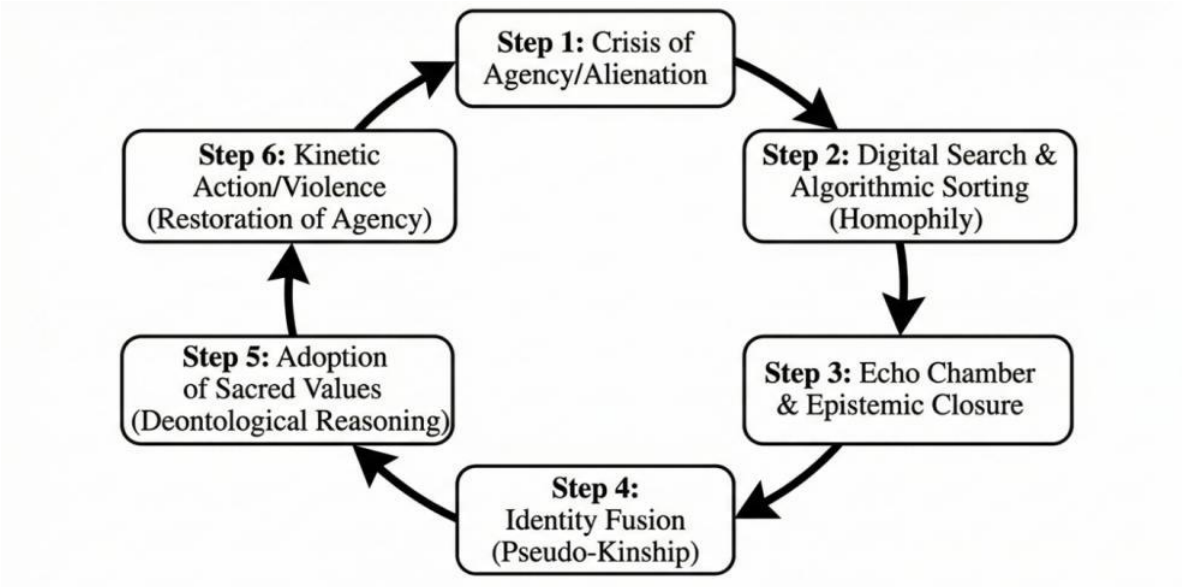
This pattern has clear implications for extremism and terrorism. Ideological tourism lowers the threshold for radicalisation because it encourages people to suspend critical judgement in exchange for belonging and certainty. Early engagement may be performative, expressed through symbols, slogans, memes and outrage rather than deep commitment. Repeated exposure to simplified narratives, hostile out-groups and emotionally charged communities can nevertheless harden into more serious identification. Single-issue movements are especially powerful because they reduce complex social problems into a single moral demand. Once that demand becomes tied to identity, compromise can feel like betrayal. Democratic politics often depends on focused campaigns, so single-issue mobilisation should not be treated as inherently extremist. Danger arises when a cause becomes a total explanation for suffering and

a substitute for wider social belonging. Under those conditions, right-wing extremism, far-left extremism, anti-state extremism, technology-related grievance movements and other radical currents can convert the search for ontological security into hostility toward democratic norms and, in a smaller number of cases, support for violence or terrorism.

5. Mechanics of Contemporary Radicalisation

Crisis of Agency

Radicalisation of the ideological tourist is best understood not as an inherent attraction to violence, but as a crisis of agency. Single-issue ideologies can provide some of the conditions of ontological security. They offer belonging, moral clarity and a sense that private distress forms part of a wider political struggle. Yet they often fail to resolve the individual's need to act meaningfully upon the world. Totalising narratives, whether focused on climate collapse, demographic replacement, state betrayal, technological threat or cultural decline, can intensify fear while making ordinary democratic action appear useless. A person caught in this position may experience high threat perception alongside low perceived agency. Such a combination is unstable because the world appears both intolerable and unchangeable. Disruptive or violent action can then become attractive, not because violence is initially desired for its own sake, but because it appears to restore control where formal politics has failed. Kinetic action proves to the individual that they still matter, can still affect events and can still impose meaning on a chaotic environment. This is especially relevant to right-wing extremism, anti-state extremism, technology-related grievance movements and other single-issue causes in which the imagined enemy is presented as existentially dangerous. Movement toward terrorism occurs when violence is reframed not as aggression, but as necessity, defence or moral duty.



Most alienated individuals never cross this threshold. Nevertheless, crisis of agency helps explain why a small minority may come to see violent extremism as the only remaining route to significance, recognition and control.

Figure 2 – Modern Radicalisation Framework: From Crisis of Agency to Kinetic Action in Six Steps

Digital Platforms as Accelerants

Digital platforms have accelerated the movement from ontological insecurity toward extremism and, in a smaller number of cases, terrorism. Political discourse now takes place inside environments designed around attention, emotional intensity and rapid group formation. These systems do not create grievance from nothing, but they can convert diffuse anxiety into communities, narratives and enemies. For the ideological tourist, online environments matter because they offer immediate access to belonging, certainty and recognition. Someone searching for meaning no longer needs to join a party, attend a meeting or study a doctrine. Entry into a digital community can provide language, symbols, validation and grievance almost instantly. Lorenz-Spreen et al. (2023) show how online environments amplify homophily – the tendency to associate with people who are similar to themselves - by encouraging users to connect with like-minded others. Repetition inside such spaces can make radical claims appear self-evident. Over time, a worldview that began as exploration may begin to feel like common sense, making digital platforms a powerful accelerant for contemporary extremism.

Attention-driven platform design reinforces this process. Content that provokes emotion, simplifies conflict and sustains engagement is often rewarded with visibility. As traditional media gatekeepers lose influence, political identity is increasingly shaped through personalised feeds, influencer networks and algorithmic recommendation. Users can also remove dissenters, block contradiction and inhabit spaces where their fears are constantly confirmed. Cinelli et al. (2021) found that homophilic clusters dominate online interaction across major platforms, while Larooij and Törnberg (2025) show how feedback loops between engagement and network growth can produce polarised communities even in relatively simple simulated platform environments. Online spaces therefore provide a synthetic form of ontological security. They reduce uncertainty by filtering out complexity, offer belonging through digital tribes and supply a clear narrative about who is responsible for suffering. Participation of this kind does not automatically lead to violence. Most users who encounter radical material never become terrorists. Even so, digital platforms can lower the threshold for extremist identification by making radical communities easy to enter, emotionally rewarding and difficult to challenge from within.

Affective Polarisation and Stochastic Terrorism

Extremism is further intensified by the affective polarisation created inside digital environments. Disagreement is not merely sharpened. It becomes emotionally organised around in-group loyalty and out-group hostility. Platform incentives contribute to this process because morally charged, simplified and provocative content can generate high levels of engagement. Matamoros-Fernández and Farkas (2021) argue that hateful or hostile content often remains visible because it attracts attention. Wagner (2024) similarly shows that citizens can become willing to discriminate on the basis of party identity, even in political systems that are only moderately polarised. Once emotional sorting takes hold, users may be repeatedly supplied with confirming evidence that their group is under threat and that opponents are dangerous, corrupt or illegitimate. Epistemic closure can then reduce uncertainty, but only by narrowing reality. A person searching for ontological security may experience radical content as reassuring rather than destabilising because it provides belonging, certainty and a clear explanation of danger.

Stochastic terrorism becomes more plausible in this environment. The term refers to a pattern in which hostile rhetoric, dehumanising narratives or repeated claims of existential threat increase the general likelihood of violence, even though the specific perpetrator and timing remain unpredictable. Angove (2024) treats the concept as emerging and contested, but it is useful here because it captures an important feature of decentralised extremism. A platform, influencer or movement does not need to instruct a particular individual to act violently. Instead, it can help produce a wider atmosphere in which lone-actor violence becomes statistically more likely. Affective polarisation, algorithmic reinforcement and sacred threat narratives all contribute to this risk by presenting opponents as enemies whose continued existence endangers the in-group. Under these conditions, the boundary between expressive outrage and violent permission can become unstable.

Yet the democratic value of digital platforms should not be overlooked. They have lowered the cost of political participation, enabled rapid mobilisation and given marginalised groups greater visibility. Bond et al. (2012) show that online social messages can increase political participation, while Mihăilescu (2024) highlights the role of political memes in anti-corruption movements and popular critique. Earl et al. (2022), however, identify a related paradox. Digital traces that enable mobilisation can also expose activists to surveillance, creating a trade-off between visibility and security. Other risks are more corrosive. NATO Strategic Communications Centre of Excellence (NATO StratCom COE, 2021), notes that online harassment and disinformation disproportionately affect women and minorities, while Hasell et al. (2024) find that repeated exposure to political attacks can increase cynicism and reduce confidence in democratic politics. Digital platforms therefore perform a double function. They can widen participation, but they can also intensify distrust, polarisation

and extremist identification. Their role in terrorism is usually indirect, but still strategically important, because they can weaken the social and cognitive conditions that make democratic compromise possible.

Active Combatants & Identity Fusion

The all-important movement from ideological tourist to active combatant requires a deeper psychological realignment. Identity fusion captures this shift by describing a condition in which the boundary between the personal self and the collective cause becomes increasingly difficult to maintain. An ideological tourist may initially engage with a movement in a transactional way, seeking belonging, certainty and relief from anxiety. A fused individual, by contrast, experiences the group as part of the self. Threats to the movement are therefore no longer interpreted as abstract political disagreements, but as personal and existential dangers. Swann et al. (2014) argue that identity fusion can produce willingness to engage in extreme pro-group behaviour, including self-sacrifice. Digital environments make this especially important because online communities can simulate the intimacy of kinship without requiring direct physical contact. Shared grievance, humiliation, humour, ritualised posting and repeated participation can make the group feel like a family, even when its members have never met. In this way, the online tribe begins to function as pseudo-kin, offering the social integration and moral certainty that the individual lacks elsewhere.

Pseudo-kinship helps explain how extremist movements turn passive support into active militancy. Martel et al. (2021) describe fused identity as a form of “visceral oneness”, in which the individual experiences the group’s fate as inseparable from their own. Once this occurs, ordinary calculations of personal risk become less decisive. Violence can be reframed as loyalty, defence or sacrifice on behalf of the collective. Identity fusion does not inevitably produce terrorism, but it lowers the psychological barriers that normally inhibit extreme action. The fused individual may come to see moral restraint as weakness and compromise as betrayal. Dangers are especially acute in right-wing extremism, anti-state extremism, technology-related grievance movements and single-issue causes where the out-group is described as an existential threat. Online pseudo-kinship therefore has serious implications for future extremist and terrorist activity because it allows dispersed individuals to experience radical causes as intimate, sacred and personally binding.

Devoted Actors and Sacred Values

A further stage occurs when identity fusion hardens into the mindset of the devoted actor. At this point, the cause is no longer treated as an ordinary political preference. It becomes a sacred value. Tetlock (2003) argues that sacred values create moral red lines that individuals believe cannot be traded, priced or compromised. Atran (2016) similarly shows that devoted actors may prioritise sacred

commitments over material incentives, personal safety or conventional cost-benefit reasoning. This marks a shift from instrumental politics to deontological reasoning, where action is judged by moral duty rather than practical consequence. Causes such as defence of the nation, protection of the climate, resistance to the state, religious duty, technological resistance or racial survival can become non-negotiable once they are sacralised. For someone experiencing ontological insecurity, this can be deeply stabilising. Sacred values reduce complexity by dividing the world into duty and betrayal, purity and corruption, loyalty and treason. They also remove the burden of continuous moral calculation because the correct course of action appears already decided by the higher cause.

Extremist movements become especially resistant to democratic containment when sacred values dominate. Ordinary politics depends on bargaining, compromise and proportionality. Sacred values resist all three. Attempts to offer material concessions may even produce a backfire effect because the devoted actor interprets compromise as moral contamination rather than reasonable negotiation. Ideology then becomes a closed system that protects the individual from uncertainty while increasing hostility toward outsiders. Not all sacred values are violent or extremist. Democratic societies also depend on deeply held commitments, including human rights, national defence and the rule of law. Danger arises when a sacred value becomes fused with an existential enemy and with the belief that violence is morally required. In that context, right-wing extremism, far-left extremism, anti-state extremism, technology-related grievance movements and other single-issue ideologies can move from protest or belief into terrorist justification. Violence is no longer seen as a strategic option alone. It becomes an obligation imposed by the sacred cause.

Kinetic Thresholds and Co-Escalation to Terrorism

Final movement from radicalised belief to terrorist violence is rarely an isolated psychological event. It is better understood as an interaction between the individual, the radical peer group and the state. Within extremist communities, status is often gained through visible commitment, risk-taking and willingness to sacrifice. Internal outbidding can follow, with members competing to show that they are more loyal, more courageous or more morally serious than others. Over time, the group’s threshold for acceptable action can shift. What initially appears extreme may become normal, while hesitation is reframed as weakness or betrayal. This matters because the devoted actor no longer evaluates action through ordinary cost-benefit reasoning. If the cause has become sacred, and if the group is experienced as pseudo-kin, then violence can be interpreted as duty rather than escalation. A person may therefore cross the kinetic threshold when violent action appears to resolve the crisis of agency, defend the in-group and prove commitment to the cause.

State action can intensify this process when it confirms the extremist narrative. Heavy-handed or indiscriminate intervention may validate the belief that the system is hostile, corrupt or fundamentally illegitimate. Honari (2018) argues that repression can crystallise injustice frames, transforming political grievance into a sharper moral struggle. Nägel and Nivette (2022) similarly suggest that state coercion may validate violence when groups interpret it as evidence that survival requires resistance. Della Porta (2018) describes this feedback loop as co-escalation, where action by the state provokes a hardened response from the movement, which then justifies further repression. In such conditions, terrorism may be reframed as defensive violence, even when it is directed against civilians or democratic institutions. Political opponents become existential enemies, and the normal mechanisms of democratic compromise are weakened. Wagner's (2024) account of affective polarisation is relevant here because hostility toward the opposing camp can become emotionally entrenched before any formal commitment to violence occurs.

Escalation is not inevitable. Stott et al. (2025) show that dialogue-based counter-terrorist policing can interrupt escalation by reducing the sense of collective threat and avoiding unnecessary validation of extremist narratives. Enforcement remains necessary where violence, intimidation or terrorist preparation is present. However, the manner of intervention matters. Poorly targeted repression can strengthen the identity fusion and sacred values that make extremist violence more likely. More precise and proportionate responses can preserve legitimacy while limiting opportunities for radical groups to claim martyrdom. Wider lessons for counter-terrorism follow directly. Terrorism often emerges when ontological insecurity, group fusion, sacred values and perceived repression combine. At that point, violence is no longer experienced by the actor as a strategic option alone, but as a morally necessary act within a closed ideological world.

6. Cognitive Warfare

Reflexive Control and the Exploitation of Ontological Insecurity

Ontological insecurity creates a strategic vulnerability as well as a domestic political risk. Rising extremism around single-issue ideologies can therefore be exploited by hostile states seeking to weaken democratic cohesion from within. Cognitive warfare targets the way citizens interpret reality, judge institutions and understand their own agency. Rather than defeating a state through conventional force, the adversary seeks to manipulate public belief, emotion and perception until self-damaging choices appear voluntary. Reflexive control is central to this approach. Thomas (2004) describes it as the use of carefully selected information to lead an opponent toward decisions that serve the interests of the initiator. In the context of democratic societies, the aim is not simply to deceive citizens, but to shape their perception of what is true, who can be trusted and which actions seem necessary.

Ontologically insecure populations are especially vulnerable because they are already searching for certainty, belonging and explanation. Hostile actors can therefore amplify existing grievances, deepen mistrust and push alienated citizens toward extremist interpretations of political life.

European experience illustrates the logic of this strategy. Lucas and Pomerantsev (2016) argue that hostile information operations often seek to delegitimise Western governments and transatlantic institutions by widening existing social divisions. Such operations rarely need to invent grievances from nothing. They work more effectively by identifying real points of alienation and intensifying them. Single-issue ideologies provide useful entry points because they already organise anxiety around clear moral claims and identifiable enemies. External actors can enter digital spaces linked to right-wing extremism, anti-state grievance, conspiracy movements, technology-related anxiety or polarised cultural issues, then amplify the most extreme voices within them. Russia's Internet Research Agency offered a clear example of this logic. Freelon and Lokot (2020) show how such operations addressed audiences through specific identity markers and sought to provoke antagonism between opposing groups. A cheap and deniable form of disruption follows. Domestic citizens become carriers of hostile influence, while the adversary supplies reinforcement, visibility and emotional acceleration. Cognitive warfare therefore turns ontological insecurity into a national security problem.

Table 3 - Operational Modalities of Modern Cognitive Warfare

Doctrine or technique	**Strategic objective**	**Mechanism of action**	**Key source**
Reflexive control	Lead the target to make choices that damage its own interests while appearing voluntary	Curated information is used to alter the target's perception of reality, available options and likely consequences	Thomas (2004)
Implausible deniability	Project power, create confusion and exhaust the adversary's capacity to respond	Operations are conducted despite likely attribution, producing uncertainty, distraction and epistemic fog	Aldrich and Cormac (2018)
Information overload	Weaken public confidence in truth, expertise and institutional authority	Large volumes of conflicting or misleading content overwhelm attention and push citizens toward simpler narratives	Centre for Emerging Technology and Security (CETAS) (2024)

Content laundering	Increase the credibility of disinformation by hiding its origin	False or misleading narratives are inserted into legitimate-looking media ecosystems, cloned websites or apparently independent sources	Democracy Reporting International (2022)
Astroturfing	Simulate public consensus and make fringe narratives appear mainstream	Bot networks, inauthentic accounts or coordinated campaigns artificially amplify selected narratives	CISA (2021)
Extremist amplification	Deepen polarisation and increase susceptibility to extremist narratives	Existing grievances linked to migration, war, public health or cultural conflict are intensified and reframed as existential threats	Lucas and Pomerantsev (2016), Europol (2024)

Information Overload and Content Laundering

Information overload is one of the main mechanisms through which cognitive warfare operates. Paul and Matthews (2016) describe the Russian “firehose of falsehood” model as high-volume, multichannel, rapid and repetitive, with little commitment to consistency or objective reality. Its effectiveness does not depend on persuading every citizen of one false claim. Instead, volume and speed make careful judgement more difficult. When people are overwhelmed by competing claims, fabricated evidence and emotional provocation, they may retreat into simpler narratives that reduce uncertainty. Generative artificial intelligence intensifies this problem by lowering the cost of producing convincing text, images, video and automated interaction. CETAS (2024) argues that these technologies are shifting influence operations from labour-intensive troll activity toward scalable automated systems. Operation Doppelgänger illustrates this development through the cloning of legitimate news domains to distribute Kremlin-aligned disinformation (U.S. Cyber Command, 2024). Its purpose is not merely to make audiences believe a particular lie. More corrosively, it weakens confidence that truth can be identified at all. Among populations already experiencing low institutional trust, information overload can accelerate movement from scepticism to cynicism, and from cynicism to extremist certainty.

Content laundering makes this process more effective by disguising the origin of manipulated narratives. Democracy Reporting International (DRI) (2022) describes the tactic as the insertion of fabricated or misleading material into more credible information ecosystems, allowing disinformation to circulate without its original source being obvious. Astroturfing then gives such narratives the appearance of public

consensus by using networks of inauthentic or coordinated accounts (Cybersecurity and Infrastructure Security Agency (CISA), 2021). During crises, these methods become especially potent because anxiety increases demand for simple explanations. Migration can be reframed as invasion, public health measures as tyranny, technological change as enslavement and foreign wars as evidence of hidden conspiracies. Georgiou and Zaborowski (2017) show how migration narratives during the 2015 refugee crisis were often framed through threat and emergency, while the EEAS (2021) documents the exploitation of COVID-19 through disinformation and the undermining of Western scientific authority. Europol (2024) similarly notes that single events can be framed in ways that appeal to different extremist audiences at once. Cognitive warfare does not create terrorism directly, but it can strengthen the narratives through which extremist movements recruit, justify hostility and normalise violence.

Artificial Intelligence and Precision Manipulation

Artificial intelligence is likely to make cognitive warfare more personalised, adaptive and difficult to detect. Earlier influence operations often relied on scale, repetition and broad audience targeting. Emerging systems can make manipulation more intimate by adapting content to an individual's fears, interests, language, identity and emotional state. CETAS (2024) warns that generative technologies may enable more scalable and persuasive forms of influence activity. In counter-terrorism terms, the risk is not only the production of more false content. Greater danger lies in the creation of synthetic environments that feel socially responsive and personally meaningful. A vulnerable individual may encounter fabricated communities, automated interlocutors, synthetic news sites or AI-generated influencers that appear to confirm their private anxieties. Where ontological insecurity already exists, such systems could provide an engineered sense of belonging, certainty and agency.

Precision manipulation would intensify the logic already described in earlier sections. The ideological tourist moves between causes in search of identity and meaning. AI-enabled influence systems could identify that search and supply increasingly tailored narratives. Someone anxious about technological displacement might be directed toward anti-technology extremism. Another person humiliated by economic failure could be steered toward racial, anti-state or conspiratorial explanations. A citizen distressed by climate change might be pushed from legitimate activism toward apocalyptic or violent interpretations. Each pathway would differ in content, but all would exploit the same psychological vulnerability. Automated systems could test which messages provoke anger, hope, fear or belonging, then adjust the narrative accordingly. Such developments would not make radicalisation automatic. Human agency, social context and offline relationships would still matter. Yet the strategic implication is clear. Hostile actors may become better able to locate moments of acute uncertainty and convert them into ideological commitment.

Institutional Responses and Epistemic Traps

Democratic states have begun to respond by building new forms of informational defence. The European Union's Digital Services Act marks one shift from voluntary platform self-regulation toward legal responsibility for systemic risks. Meyers (2022) argues that this reflects a broader change in how states approach online harms. Specialist institutions, including the EU's East StratCom Task Force and NATO StratCom COE, also show growing recognition that the cognitive domain has become a security environment in its own right. Yet democratic responses face a serious dilemma. Too little action leaves hostile actors and extremist movements free to exploit the information space. Excessive or poorly explained intervention risks making the state appear to police truth, suppress dissent or protect elite interests. In a low-trust environment, attempts to regulate harmful but lawful content can therefore be interpreted as censorship rather than protection.

Bateman and Jackson (2024) warn that state interventions in contested information environments can be read as partisan acts, even when presented as neutral safeguards. Hostile actors can then exploit the intervention itself as proof that democratic governments fear the truth. Extremist movements use the same logic. Right-wing extremism, anti-state activism and conspiracy-based movements can portray moderation, fact-checking or platform regulation as evidence of persecution. A self-reinforcing crisis follows, in which every corrective measure risks becoming further material for distrust. Democratic states should not therefore abandon regulation, but informational defence must be transparent, proportionate and rooted in institutional legitimacy. The deeper problem is not only false content. It is the erosion of shared reality. Once citizens no longer trust any common account of events, democratic compromise becomes harder and extremist narratives become more attractive.

Strategic Implications for Counter-Terrorism

Cognitive warfare changes the counter-terrorism problem because it blurs the boundary between domestic radicalisation and external manipulation. Extremist narratives may arise from real local grievances, circulate through domestic digital communities and then be amplified by hostile states for strategic effect. Attribution can therefore be difficult. A violent actor may be domestic, while the emotional and informational environment surrounding them has been shaped partly by foreign influence. This does not mean that every extremist movement is foreign-directed. Such a claim would be analytically weak and politically dangerous. Rather, hostile states can exploit the same conditions that make extremist narratives attractive in the first place. Ontological insecurity, declining trust, political exclusion and digital fragmentation become force multipliers for adversarial influence.

Counter-terrorism must therefore treat cognitive resilience as part of national security. Intelligence, policing and platform regulation remain necessary, but they cannot by themselves repair the social and psychological vulnerabilities that hostile actors exploit. If cognitive warfare works by manipulating citizens' difficulty in interpreting complex digital environments, then democratic resilience requires systematic preparation for reasoning under informational pressure. Education becomes strategically important for this reason. Citizens need the capacity to recognise manipulation, tolerate uncertainty, evaluate evidence and resist the emotional comfort of totalising explanations. Such preparation should not be treated as a narrow school policy or as a soft alternative to security. It is a practical counter-terrorism measure because it reduces the susceptibility of citizens to radicalisation, disinformation and AI-enabled targeting. The next section therefore turns from diagnosis to policy, arguing for a National E-Education Strategy grounded in critical reasoning, digital literacy and civic resilience.

7. Conclusions and Policy Prescriptions

Future terrorism and extremism must be understood within a wider crisis of ontological security. Previous sections have argued that many contemporary radical movements do not gain influence simply because their doctrines are persuasive. They gain influence because they offer belonging, agency and meaning to individuals who experience mainstream society as unstable, illegible or closed. Declining religious authority, failed totalitarian substitutes, consumer individualism, neoliberal agency erosion and the collapse of trust after the financial crisis have all contributed to this condition. None of these developments automatically produces terrorism. Rather, they create an environment in which extremist narratives can become more attractive, especially when they promise certainty, restored control and moral purpose. Right-wing extremism, far-left extremism, anti-state extremism, technology-related grievance movements and single-issue ideologies all exploit this vulnerability by reducing complexity, identifying enemies and giving alienated individuals a role inside a wider struggle.

Fragmentation is therefore likely to define the future threat environment. Tomorrow's ideological terrorist may not emerge from a stable organisation with a coherent doctrine. Instead, they may pass through a sequence of online communities, grievances and single-issue causes before settling temporarily on the narrative that best satisfies their need for certainty and agency. Digital platforms accelerate this process by creating synthetic communities, reinforcing affective polarisation and transforming political claims into sacred values. Hostile states can then exploit these domestic vulnerabilities through cognitive warfare, disinformation, reflexive control and AI-enabled manipulation. Ontological insecurity becomes a national security concern because it allows external actors to manipulate internal fractures without crossing a physical border.

By 2042, this threat may become more personalised and adaptive. Current influence operations already use scale, speed and emotional intensity to overwhelm public judgement. Future systems may move further toward precision manipulation, using artificial intelligence to identify and exploit moments of anxiety, loneliness, humiliation or despair. Drawing on research exploring cognitive warfare and AI-enabled influence operations, it is plausible that hostile actors will increasingly use synthetic forums, fabricated news environments, automated influencers and AI companions to create closed informational worlds around vulnerable individuals. Such systems would not make radicalisation automatic, but they could make extremist narratives feel more intimate, coherent and personally responsive. Under these conditions, the state can be framed as an enemy, violence as duty and terrorism as restored agency.

Counter-terrorism cannot therefore rely only on disruption, surveillance and prosecution. These tools remain necessary, especially where violence, intimidation or terrorist preparation is present. Yet they address the endpoint of radicalisation more than the conditions that make extremist narratives persuasive. A more durable response requires democratic states to strengthen the cognitive, civic and social resilience of the population. Such work should not be dismissed as soft prevention or as a narrow educational concern. It is part of national security because hostile actors and extremist movements both exploit the same vulnerabilities, including low trust, poor digital literacy, social isolation, agency loss and difficulty reasoning under informational pressure.

A National E-Education Strategy should form one practical response. This must not be treated as a narrow school policy, but as a population-level resilience programme extending across education, further and higher education, adult learning, public information and professional training. Its purpose would not be to tell citizens what to think. Instead, it would strengthen their capacity to think under pressure, tolerate uncertainty, evaluate evidence and recognise manipulation. Citizens need to understand why simple answers feel emotionally attractive, why digital communities can become psychologically binding and why algorithmic environments can intensify outrage, certainty and identity fusion. In counter-terrorism terms, this is preventive infrastructure. A population better able to reason under pressure is less vulnerable to radicalisation, disinformation and hostile-state manipulation.

Three connected pillars should structure the strategy. Foundations of inquiry would give learners a basic understanding of evidence, uncertainty, disagreement and the psychological comfort offered by simple answers. Applied critical reasoning would develop the ability to identify emotional manipulation, logical fallacies, conspiracy structures, false moral binaries and claims that turn ordinary political disagreement into existential threat. Digital ecosystem literacy would move beyond basic technical competence to explain how platforms shape attention, recommendation, status,

outrage and belonging. Chung and Wihbey (2024) identify continuing gaps in public understanding of algorithmic systems, while Edwards et al. (2024) argue that democratic citizens require stronger forms of digital literacy to navigate the European information environment. Together, these pillars would help citizens recognise when political communication is informing them, recruiting them or manipulating them.

Policy design must also avoid the epistemic trap identified in the previous section. A resilience strategy will fail if it appears to impose an official truth or delegitimise dissent. Democratic societies depend on protest, disagreement and single-issue campaigns. The aim should therefore be to protect the conditions of democratic judgement rather than prescribe acceptable opinion. Transparency, pluralism and independence are essential. Educational materials should distinguish clearly between lawful dissent, extremism and terrorist justification. They should also make explicit that scepticism toward government is not itself a security threat. Danger arises when distrust hardens into a closed worldview in which opponents become existential enemies, compromise becomes betrayal and violence becomes morally required.

Wider civic renewal is also necessary. E-education can strengthen individual resilience, but it cannot fully compensate for social isolation, economic insecurity or the absence of meaningful participation. Democratic states must therefore rebuild credible non-extremist sources of belonging, agency and meaning. This includes accessible political participation, trusted local institutions, community infrastructure, youth engagement, fairer routes into adulthood and public services that make the state feel legible rather than distant. Citizens who possess stronger ontological security are less likely to seek certainty in radical movements and less vulnerable to hostile manipulation. Counter-terrorism should therefore be understood not only as a matter of stopping plots, but also as the defence of the social and cognitive conditions that allow democratic life to continue.

The future of counter-terrorism will depend partly on whether democratic societies can make the world feel more intelligible, participation more meaningful and agency more real. Extremism and terrorism flourish when individuals experience life as chaotic, humiliating and closed. A resilient democracy should not recreate religious authority, impose a single national doctrine or suppress legitimate dissent. Its task is to build the civic, educational and digital conditions in which disagreement can survive without collapsing into existential hostility. Where citizens have belonging without tribalism, agency without violence and meaning without fanaticism, extremist narratives lose much of their appeal.

References

Adam-Troian, J., Tecmen, A. and Kaya, A. (2021) ‘Youth extremism as a response to global threats? A threat-regulation perspective on violent extremism among the youth’, *European Psychologist*, 26(1), pp. 15–28. Available at: https://doi.org/10.1027/1016-9040/a000415

Aldrich, R.J. and Cormac, R. (2018) ‘Grey is the new black: covert action and implausible deniability’, *International Affairs*, 94(3), pp. 477–494. Available at: https://doi.org/10.1093/ia/iiy067.

Angove, J.M. (2024) ‘Stochastic terrorism: critical reflections on an emerging concept’, *Critical Studies on Terrorism*, 17(1), pp. 1–22. Available at: https://doi.org/10.1080/17539153.2024.2305742

Arundel, R. and Hochstenbach, C. (2021) ‘Housing unaffordability and mental health: A longitudinal analysis of private renters and homeowners’, *Housing Studies*, 39(2), pp. 336–356. Available at: https://doi.org/10.1080/02673037.2022.2109289.

Atran, S. (2016) ‘The Devoted Actor: Unconditional Commitment and Intractable Conflict across Cultures’, *Current Anthropology*, 57(S13), pp. S192–S203. Available at: https://doi.org/10.1086/685495.

Autor, D., Dorn, D. and Hanson, G.H. (2021) *On the persistence of the China shock*. NBER Working Paper No. 29401. Cambridge, MA: National Bureau of Economic Research. Available at: https://doi.org/10.3386/w29401.

Bateman, J. and Jackson, D. (2024) *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Washington, D.C.: Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide (Accessed: 2 October 2025).

Bauman, Z. (2007) *Consuming Life*. Cambridge: Polity Press.

Berman, S. and Snegovaya, M. (2019) ‘Populism and the Decline of Social Democracy’, *Journal of Democracy*, 30(3), pp. 5–19. Available at: https://doi.org/10.1353/jod.2019.0038.

Bird-David, N. (1999) ‘“Animism” Revisited: Personhood, Environment, and Relational Epistemology’, *Current Anthropology*, 40(S1), pp. S67–S91.

Bond, R.M. et al. (2012) ‘A 61-million-person experiment in social influence and political mobilization’, *Nature*, 489(7415), pp. 295–298. Available at: https://doi.org/10.1038/nature11421.

Bresser-Pereira, L.C. (2010) ‘The global financial crisis and a new capitalism?’, *Journal of Post Keynesian Economics*, 32(4), pp. 499–534. Available at: https://doi.org/10.2753/PKE0160-3477320401.

Carpenter, M.J. and Perrier, B. (2023) ‘Yellow Vests: Anti austerity, prodemocracy, and popular (not populist)’, *Frontiers in Political Science*, 5, p. 1037942. Available at: https://doi.org/10.3389/fpos.2023.1037942.

Case, A. and Deaton, A. (2020) *Deaths of Despair and the Future of Capitalism*. Princeton: Princeton University Press.

Centre for Emerging Technology and Security (CETAS) (2024) *AI-enabled influence operations: Safeguarding future elections*. London: The Alan Turing Institute. Available at: https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections (Accessed: 2 October 2025).

Chung, M. and Wihbey, J. (2024) ‘The algorithmic knowledge gap within and between countries: Implications for combatting misinformation’, *Harvard Kennedy School (HKS) Misinformation Review*, 5(4). Available at: https://doi.org/10.37016/mr-2020-131.

Cinelli, M. et al. (2021) ‘The echo chamber effect on social media’, *Proceedings of the National Academy of Sciences*, 118(9), p. e2023301118. Available at: https://doi.org/10.1073/pnas.2023301118.

Coan, J.A. and Sbarra, D.A. (2015) ‘Social Baseline Theory: The Social Regulation of Risk and Effort’, *Current Opinion in Psychology*, 1, pp. 87–91.

Cox, C. and Shapiro, I. (2025) ‘Party realignment and single-issue voters’, *PLOS ONE*, 20(3), p. e0319522. Available at: https://doi.org/10.1371/journal.pone.0319522.

Crawford, J. (2015) ‘The Moral Hazard Paradox of Financial Safety Nets’, *Cornell Journal of Law and Public Policy*, 25(1), pp. 1–56. Available at: https://ssrn.com/abstract=2580062 (Accessed: 2 October 2025).

Cybersecurity and Infrastructure Security Agency (CISA) (2021) *Tactics of Disinformation*. Washington, D.C.: CISA. Available at: https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf (Accessed: 2 October 2025).

Della Porta, D. (2018) ‘Radicalization: A Relational Perspective’, *Annual Review of Political Science*, 21, pp. 461–474. Available at: https://doi.org/10.1146/annurev-polisci-042716-102314.

Democracy Reporting International (DRI) (2022) *ON THE RADAR: Mapping the Tools, Tactics and Narratives of Tomorrow’s Disinformation Environment*. Berlin: DRI. Available at: https://democracyreporting.s3.eu-central-1.amazonaws.com/images/62c8333ec3aea.pdf (Accessed: 2 October 2025).

Dunbar, R.I.M. (1992) ‘Neocortex size as a constraint on group size in primates’, *Journal of Human Evolution*, 22(6), pp. 469–493.

Durkheim, E. (1951) *Suicide: A Study in Sociology*. Translated by J.A. Spaulding and G. Simpson. Glencoe, IL: Free Press. (Original work published 1897).

Earl, J., Maher, T.V. and Pan, J. (2022) 'The digital repression of social movements, protest, and activism: A synthetic review', *Science Advances*, 8(10), p. eabl8198. Available at: https://doi.org/10.1126/sciadv.abl8198.

Edelman (2024) *Edelman Trust Barometer 2024: Global Report*. Available at: https://www.edelman.com/trust/2024/trust-barometer (Accessed: 2 October 2025).

Edwards, L., Livingstone, S. and Goodman, E. (2024) *Putting media literacy on the map: opportunities and challenges in Europe*. Media@LSE. Available at: https://blogs.lse.ac.uk/medialse/2024/12/03/putting-media-literacy-on-the-map-opportunities-and-challenges-in-europe/ (Accessed: 2 October 2025).

European External Action Service (EEAS) (2021) *EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic (Update December 2020 - April 2021)*. Available at: https://www.eeas.europa.eu/delegations/georgia/eeas-special-report-update-short-assessment-narratives-and-disinformation-around-covid-19-pandemic_en?s=221 (Accessed: 17 October 2025).

Europol (2024) *European Union Terrorism Situation and Trend Report 2024*. Luxembourg: Publications Office of the European Union. Available at: https://doi.org/10.2813/50085.

Fiva, J.H., Izzo, F. and Tukiainen, J. (2024) 'The gatekeeper's dilemma: Political selection or team effort', *Journal of Public Economics*, 234, p. 105133. Available at: https://doi.org/10.1016/j.jpubeco.2024.105133.

Frankl, V.E. (1984) *Man's Search for Meaning*. New York: Washington Square Press. (Original work published 1946).

Freelon, D. and Lokot, T. (2020) 'Russian disinformation campaigns on Twitter target political communities across the spectrum', *Harvard Kennedy School Misinformation Review*, 1(1). Available at: https://doi.org/10.37016/mr-2020-003.

Friston, K. (2010) 'The free-energy principle: a unified brain theory?', *Nature Reviews Neuroscience*, 11(2), pp. 127–138.

Fukuyama, F. (1992) *The End of History and the Last Man*. New York: Free Press.

Gallup & Walton Family Foundation (2025) *Gen Z Is Using AI but Reports Gaps in School and Workplace Support*. Walton Family Foundation and GSV Ventures. Available at: https://www.waltonfamilyfoundation.org/about-us/newsroom/gen-z-is-using-ai-but-reports-gaps-in-school-and-workplace-support (Accessed: 18 October 2025).

Giddens, A. (1991) *Modernity and Self-Identity – Self and Society in the Late Modern Age*. Cambridge, Polity Press.

Georgiou, M. and Zaborowski, R. (2017) *Media coverage of the "refugee crisis": A cross-European perspective*. Strasbourg: Council of Europe. Available at: https://rm.coe.int/1680706b09 (Accessed: 2 October 2025).

Harrison, M. (2001) *Are Command Economies Unstable? Why did the Soviet Economy Collapse?* The Warwick Economics Research Paper Series (TWERPS) 604. Coventry: University of Warwick. Available at: https://warwick.ac.uk/fac/soc/economics/research/workingpapers/2001/twerp_604.pdf (Accessed: 2 October 2025).

Hasell, A., Halversen, A. and Weeks, B. (2024) 'When Social Media Attack: How Exposure to Political Attacks on Social Media Promotes Anger and Political Cynicism', *The International Journal of Press/Politics*, 30(1), pp. 1–23. Available at: https://doi.org/10.1177/19401612231221806.

Hayes, G. et al. (2024) 'Extinction Rebellion's disobedient environmental citizenism', *Environmental Politics*, 34(5), pp. 817–836. Available at: https://doi.org/10.1080/09644016.2024.2406183.

Hickman, C. et al. (2021) 'Climate anxiety in children and young people and their beliefs about government responses to climate change: A global survey', *The Lancet Planetary Health*, 5(12), pp. e863–e873. Available at: https://doi.org/10.1016/S2542-5196(21)00278-3.

Honari, A. (2018) 'From "the effect of repression" toward "the response to repression"', *Current Sociology*, 66(6), pp. 950–973. Available at: https://doi.org/10.1177/0011392118787585.

Jakobsen, L. (2024) *Examining donations ahead of European elections*. European Democracy Consulting. Available at: https://eudemocracy.eu/examining-donations-ahead-of-european-elections (Accessed: 2 October 2025).

Konczal, M., Milani, K. and Evans, A. (2020) *The empirical failures of neoliberalism*. New York: Roosevelt Institute. Available at: https://rooseveltinstitute.org/wp-content/uploads/2020/07/RI_The-Empirical-Failures-of-Neoliberalism_brief-202001.pdf (Accessed: 2 October 2025).

Larooij, M. and Törnberg, P. (2025) *Can We Fix Social Media? Testing Prosocial Interventions using Generative Social Simulation*. arXiv:2508.03385. Available at: https://arxiv.org/abs/2508.03385 (Accessed: 2 October 2025).

Lennartz, C., Arundel, R. and Ronald, R. (2015) 'Younger adults and homeownership in Europe through the Global Financial Crisis', *Population, Space and Place*, 22(8), pp. 823–835. Available at: https://doi.org/10.1002/psp.1961.

Locke, J. (1983) *Two Treatises of Government*. Edited by P. Laslett. Cambridge: Cambridge University Press. (Original work published 1689).

Lorenz-Spreen, P. et al. (2023) 'A systematic review of worldwide causal and correlational evidence on digital media and democracy', *Nature Human Behaviour*, 7, pp. 74–101. Available at: https://doi.org/10.1038/s41562-022-01460-1.

Lucas, E. and Pomerantsev, P. (2016) *Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. Washington, D.C.: Centre for European Policy Analysis. Available at:

https://cepa.org/wp-content/uploads/2020/11/CEPA-Report-Winning-the-Information-War.pdf (Accessed: 2 October 2025).

Martel, F.A. et al. (2021) ‘Why True Believers Make the Ultimate Sacrifice: Sacred Values, Moral Convictions, or Identity Fusion?’, *Frontiers in Psychology*, 12, p. 779120. Available at: https://doi.org/10.3389/fpsyg.2021.779120.

Matamoros-Fernández, A. and Farkas, J. (2021) ‘Racism, Hate Speech, and Social Media: A Systematic Review and Critique’, *Television & New Media*, 22(2), pp. 205–224. Available at: https://doi.org/10.1177/1527476420982230.

McEwen, B.S. (1998) ‘Protective and damaging effects of stress mediators’, *New England Journal of Medicine*, 338(3), pp. 171–179.

Melios, G. (2020) *Europe in crisis: Political trust, corruption and austerity*. London: UCL Institute for Global Prosperity. Available at: https://www.ucl.ac.uk/bartlett/sites/bartlett/files/europe_in_crisis_0.pdf (Accessed: 2 October 2025).

Meyers, Z. (2022) *Will the Digital Services Act save Europe from disinformation?* London: Centre for European Reform. Available at: https://www.cer.eu/insights/will-digital-services-act-save-europe-disinformation (Accessed: 2 October 2025).

Mihăilescu, M.G. (2024) ‘Meme-Ing Waves: unpacking political narratives in the Romanian context’, *Journal of Contemporary Central and Eastern Europe*, 32(3), pp. 551–578. Available at: https://doi.org/10.1080/25739638.2024.2426330.

Mishler, W. and Rose, R. (2001) ‘What Are the Origins of Political Trust?: Testing Institutional and Cultural Theories in Post-communist Societies’, *Comparative Political Studies*, 34(1), pp. 30–62. Available at: https://doi.org/10.1177/0010414001034001002.

Mitzen, Jennifer (2006) "Ontological security in world politics: State identity and the security dilemma." *European journal of international relations* 12.3: 341-370.

Nägel, C. and Nivette, A. (2022) ‘Protest policing and public perceptions of police. Evidence from a natural experiment in Germany’, *Policing and Society*, 33(1), pp. 64–80. Available at: https://doi.org/10.1080/10439463.2022.2064857.

NATO Strategic Communications Centre of Excellence (2021) *Abuse of Power: Coordinated Online Harassment of Finnish Government Ministers*. Riga: NATO StratCom COE. Available at: https://stratcomcoe.org/publications/abuse-of-power-coordinated-online-harassment-of-finnish-government-ministers/5 (Accessed: 2 October 2025).

Newman, N. et al. (2024) *Reuters Institute Digital News Report 2024*. Oxford: Reuters Institute for the Study of Journalism. Available at: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024 (Accessed: 2 October 2025).

OECD (2024) *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results: Building Trust in a Complex Policy Environment*. Paris: OECD Publishing. Available at: https://doi.org/10.1787/9a20554b-en.

Paul, C. and Matthews, M. (2016) *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica, CA: RAND Corporation. Available at: https://www.rand.org/pubs/perspectives/PE198.html

Pew Research Centre (2024) *Public Trust in Government: 1958-2025*. Washington, D.C.: Pew Research Centre. Available at: https://www.pewresearch.org/politics/2025/12/04/public-trust-in-government-1958-2025/ (Accessed: 2nd October 2025).

Pew Research Centre (2024) *Satisfaction with democracy has declined in recent years in high-income nations*. Washington, D.C.: Pew Research Centre. Available at: https://www.pewresearch.org/short-reads/2024/06/18/satisfaction-with-democracy-has-declined-in-recent-years-in-high-income-nations/ (Accessed: 2 October 2025).

Putnam, R.D. (2000) *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.

Rickard, S. (2017) 'Electoral Systems and Policy Outcomes', *Oxford Research Encyclopaedia of Politics*. Available at: https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-267 (Accessed: 17 October 2025).

Royall, F. (2019) 'The Gilets Jaunes protests: mobilisation without third-party support', *Modern & Contemporary France*, 28(1), pp. 99–118. Available at: https://doi.org/10.1080/09639489.2019.1676217.

Ryan, R.M. and Deci, E.L. (2001) 'On happiness and human potentials: A review of research on hedonic and eudaimonic well-being', *Annual Review of Psychology*, 52, pp. 141–166.

Stansbury, A. and Summers, L.H. (2020) 'Declining worker power and American economic performance', *Brookings Papers on Economic Activity*, Spring, pp. 1–96.

Starostin, M. (2025) *Flash Eurobarometer 3392 (Youth Survey 2024)*. Brussels: European Parliament. Available at: https://europa.eu/eurobarometer/surveys/detail/3392 (Accessed: 2 October 2025).

Stott, C. et al. (2025) 'The Columbus model: crowd psychology, dialogue policing and protest management in the U.S.A.', *Policing and Society*. Available at: https://doi.org/10.1080/10439463.2025.2532546.

Swann, W.B. Jr. et al. (2014) 'What makes a group worth dying for? Identity fusion fosters perception of familial ties, promoting self-sacrifice', *Journal of Personality and Social Psychology*, 106(6), pp. 912–926.

Tetlock, P.E. (2003) 'Thinking the unthinkable: sacred values and taboo cognitions', *Trends in Cognitive Sciences*, 7(7), pp. 320–324.

Thomas, T.L. (2004) ‘Russia’s Reflexive Control Theory and the Military’, *The Journal of Slavic Military Studies*, 17(2), pp. 237–256. Available at: https://doi.org/10.1080/13518040490450529.

Tooze, A. (2018) *Crashed: How a decade of financial crisis changed the world*. London: Allen Lane.

Turner, A. (2015) ‘Generation Z: Technology and social interest’, *The Journal of Individual Psychology*, 71(2), pp. 103–113. Available at: https://doi.org/10.1353/jip.2015.0021.

U.S. Cyber Command (USCYBERCOM) (2024) ‘Russian Disinformation Campaign “DoppelGänger” Unmasked: A Web of Deception’, *U.S. Cyber Command News*, 3 September. Available at: https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/ (Accessed: 2 October 2025).

Wagner, M. (2024) ‘Affective polarization in Europe’, *European Political Science Review*, 16(3), pp. 378–392. Available at: https://doi.org/10.1017/S1755773923000383.

Walgrave, S., Wouters, R. and Lefevere, J. (2022) ‘Turning the heat on: The agenda-setting effect of protest on television news’, *Political Communication*, 39(1), pp. 1–21. Available at: https://doi.org/10.1080/10584609.2021.1965218.

Wike, R. et al. (2019) *European Public Opinion Three Decades After the Fall of Communism*. Washington, D.C.: Pew Research Center. Available at: https://www.pewresearch.org/global/2019/10/15/european-public-opinion-three-decades-after-the-fall-of-communism/ (Accessed: 2 October 2025).

CHAPTER 9

Online Intervention Strategies for Preventing Youth Radicalization

Dr. Erin Saltman

Abstract

Advancing technologies allow for increasingly personalized online experiences across platforms and a youth generation continuously at the forefront of digital fluency. Younger audiences are building communities, creatively expressing themselves, and finding psychosocial support through online mediums. This fast-moving dynamism has raised concerns by parents, educators, and policy makers trying to ensure adequate online safety parameters in a space they are less fluent in. In the past decade, there has been an increase in younger lone attacker terrorist perpetrators and signs of recruitment and radicalization of young audiences across a wide array of platforms and various violent extremist ideologies. In parallel, technology companies are launching new hybrid methods for scaled moderation and enforcement, including in the prevention space. This includes new AI-led detection tools and predictive behavioral models. This chapter looks at the advancing technologies and online infrastructures and compares this with known and developing tactics for preventing and countering terrorism and violent extremism online. With a specific lens on youth-focused frameworks and initiatives, this chapter predicts where online interventions to prevent youth radicalization could evolve to, what ethical considerations need to be enforced, and what will be needed for adequate targeted and scaled tactics in this space, arguing for a robust cross-sector effort that is currently lacking.

Introduction

As technology rapidly evolves, so too do the threats and opportunities brought by each advancement. Artificial intelligence (AI) is being integrated into an increasing number of platforms and products, and a younger generation is fluidly and fluently engaging with a myriad of online spaces including social media, gaming, education apps, and virtual marketplaces. While youth safety continues to be a large focus for governments, attention is also being drawn to the increasing number of criminal investigations and arrests of younger perpetrators under terrorism and violent extremism (TVE) charges. In recent years, youth arrests with significant digital

footprints have been noted in the UK [2], Canada[3], across Europe[4], in West Africa (UNODC 2017), and highlighted as a key Five Eyes Government insight of concern (Five Eyes Insights 2024). Meanwhile the digital generation divide is seeming to widen. Parents, educators, and policy makers are trying to ensure adequate online safety parameters in digital spaces they are often less fluent in. Calls for greater online safety efforts for young people naturally means a greater focus on digital resilience, prevention, and counter-extremism programming, including through the deployment of online interventions tactics. While much has been done to prevent and counter violent extremism (PCVE) online, this chapter argues that a new wave of tech tool integration and partnership models is needed, including cross-platform approaches, to scale the impact of these efforts to ensure adequate youth safety across the digital landscape.

Positive interventions online can include a wide range of approaches such as counter-narrative campaigns, digital literacy treatments, and redirection tactics. It can take many forms across a variety of online spaces. Positive intervention work online grew substantively throughout the 2010s and spread to a wider range of online platforms in the early 2020s. The concept and deployment of preventing and countering violent extremism online peaked between 2013 and 2020 when the religiously extremist terrorist organization, DAESH, grew to its highest global relevance. This was followed by the white supremacy motivated Christchurch Mosque attacks in New Zealand in 2019, and a subsequent wave of lone actors livestreaming their attacks in the US, Germany, Türkiye, Russia, India and elsewhere (GIFCT Transparency Report 2025). These trends highlighted the integration of online exploitation as a TVE tactic and led governments, the private sector, and wider civil society to align on calls for fast remedial action. This alignment meant that significant government and private sector resources were deployed without criticism. Support for civil society organizations and activist groups to counter online terrorism and violent extremism was numerous and international (Saltman and Zamir, 2024).

Many lessons have been learned, tactics evolved, and evaluation frameworks advanced. Some platforms and organizations have continued to innovate and explore new vectors for positive interventions. However, while online counterterrorism efforts have continued to grow in most cases, the global expansion of positive intervention frameworks has in some cases stalled, with many public-private partnership models

[2] In 2023, 19% (42 out of 219) of total terrorist arrests under terrorist charges in the UK were perpetrators under the age of 17 (Counter Terrorism Policing 2024).

[3] Between April 2023 and March 2024, the Royal Canadian Mounted Police reported an increase in terrorist charges and arrests with a notable increase of 17 underage, youth, and young adult suspects and perpetrators (Bell & Akin 2025).

[4] A report by the European Union reviewed terrorist arrests in 2023, noting that young people were involved in planning attacks, developing and distributing propaganda, and inciting violence. The report pointed to concerns of exploitation through virtual communities that reinforced extremist views and targeted young people with visually appealing content (European Parliament 2025).

scaling back, despite the evidence pointing to an increasingly vulnerable youth population. Some of the key aspects affecting this are as simple as the age-old questions of defining terrorism and violent extremism. Outside of groups like Al Qaeda and DAESH, Governments do not have clearly agreed TVE frameworks to rally resources and subsequently, tech companies are often given conflicting messages on definitions and priorities. New trends of nihilistic, sadistic, and misogyny based violent extremism targeting youth audiences online often fall between the gaps of government designations. Adding a youth dimension to this work adds further complexity with the diversification of platforms being used and an age divide between the platforms or parents and those of a younger generation.

This chapter maps the state-of-play in tooling, explores innovations in positive intervention tactics, identifies the current blockers for scaled deployment, and highlights what is needed to advance effective online interventions preventing youth radicalization. It is informed by case studies, trends analysis, and information exchanged during the 2025 Working Group on *Addressing Youth Radicalization and Mobilization* of the Global Internet Forum to Counter Terrorism (GIFCT).

Understanding Online Signals: Effective Audience Segmentation & Positive Interventions

The ability to identify harmful activities online has increased exponentially in the last decade. This trend is set to increase further as open sourced and decentralized access to AI and machine learning tools allows a wider variety of platforms to increase their trust and safety efforts. While early audience segmentation relied on rudimentary platform information such as age and location, the ability to detect a diversity of online harms signals has a direct impact on the potential to deploy nuanced and effective counter measures, including positive interventions (Braddock 2020, Zamir 2022). The type of signals platforms are able to track also influences the ability to advance measurement and evaluation of positive intervention tactics. This section looks at three levels for tracking terrorist and violent extremist harm signals online, how this can be used for audience segmentation, and the impact this has on the measurement and evaluation of online interventions.

When developing programmatic efforts to prevent and counter terrorism and violent extremism online, audience segmentation is critical so that the intended campaign or treatment reaches the audience it is intended for. Audience targeting traditionally requires a significant amount of research and community engagement. While this remains significant, if the online likes, interests, engagements, and behaviors of someone links them to being at risk or vulnerable to TVE networks, this data can assist in segmentation to offer the positive intervention the best chance of engagement and impact with the right target audience (Zamir 2022, Playbook on Positive Intervention Strategies 2023). The more that is known about an online

audience, the more positive intervention messaging can land in a relevant, relatable, and impactful way. For broad resilience and prevention work with younger audiences, the aim will be to reach a wide audience and build awareness and sensitivities so that a youth audience is less prone to find TVE content or activities alluring in the first place and possibly has tools to flag when they do see this content. This sort of campaign might target a whole city or country of young people within a certain age bracket, However, as efforts grow to add layered nuance to understanding segments of at-risk youth populations, and better understand if someone might already be on a spectrum of radicalization, refined audience segmentation is needed (Saltman et al 2021).

Three primary layers of user signal that can assist audience segmentation online are (1) content signals, (2) behavioral signals, and (3) network signals. Each in turn has the potential to be used reactively to deploy different positive interventions online.

	Content Signal	Behavioural Signal	Network Signal
Ads Targeting	Specific Content Violation → Targeted Ads Campaign	Violating behavior linked to harm type → Targeted Ads Campaign	Identified relation to harmful network → Targeted Ads Campaign
Search Redirect		User search for known phrases/terms linked to harm type → Search Redirection to alternative content/outlets	
Violation-Based Content Surfacing	Specific Content Violation → In feed series of counter or alternative content	Violating behavior linked to harm type → In feed series of counter or alternative content	Identified relation to harmful network → In feed series of counter or alternative content
Strategic Network Disruptions			Identified relation to harmful network → Removal of core network and counter or alternative content treatment to peripheral network
AI Chatbot Disengagement Support		Violating behavior linked to harm type → Offer to engage support bot	Identified relation to harmful network → Offer to engage support bot

Figure 1. Harm Signal Types and Corresponding Positive Intervention Options

This table maps which terrorist or violent extremist harm signal produced by a user could effectively initiate a specific type of positive intervention tactic by a platform in order to prevent and/or counter the harmful behavior or activity. The intervention types are discussed further in the following sections.

Content Signals

Content signals can vary depending on the type of platform where young audiences have potential exposure to harmful groups or individuals. Examples of content signals in social media could be that an online user has posted or reshared images or videos that have been flagged and removed under TVE or wider "Dangerous Organization" policies. This might not be severe enough to have a user's profile banned but serves as a content indicator that the user has an affinity or affiliation to a TVE group or ideology. In gaming spaces online content signals might be a user taking on a user handle, or a variation of a character name indicating an interest in TVE figures (e.g. Adolf Hitler, Brenton Tarrant, Anders Breivik, Osama Bin Laden). In online gaming spaces this might also be signal from character modification choice (e.g. dressing a character akin to a terrorist or using iconography from a TVE groups) including world building choices (e.g. drawing or building elements that relate to a TVE group such as usage of swastikas or DAESH flag references) (Kowert & Chittick 2025, Lamphere-Englund 2025).

Even with clear TVE content signal context in these cases matters and false-positives should be accounted for. Many academics, experts, and mainstream media outlets share TVE content in relation to their analysis or coverage of a topic, yet wouldn't be considered sympathetic towards the group, despite sharing the content. Often, particularly younger audiences, might find it funny or subversive to take on the name of a terrorist or attacker in military simulation games without thinking of the action being a pledge of support to the affiliated group or figure. Content signal is one layer of threat detection that can inform a platform that an online user might be at risk, or already sympathetic, with a TVE entity. Content signals can also inform behavioral activity.

Behavioral Signals

Behavioral signals include online user activities such as likes, interests, and engagements online (CAPPI: Positive Interventions 2021). These can be agnostic of a user's own content creation or posting habits. The posts or content from other users that an individual consumes and reacts to can sometimes say more about the person's sociopolitical beliefs than the content they themselves might develop or post. Particularly for younger audiences, the influencers they follow and content they consume can say a lot about early ideological sympathies (UNODC 2017). How online

behaviors might shift over time can also show a user might go from banal to higher risk.

There has been a growing concern by governments and certain civil society groups about youth consumption of what might be considered “borderline content”. Often this refers to content that is not policy violating but has fringe connections or sympathies to TVE networks or material (Saltman & Hunt 2023). While this content is difficult to define and label at scale, the tracking of youth engagement with this content can segment an online user base for positive intervention treatments. Behavioral signals might also look like swarmcasting or online activism whereby a group takes action or comments around particular targeted groups or individuals online. The behavior can look like bullying, grooming, or coordinated activism. At this point a series of behaviors can assist in identifying a wider harm-based network.

Network Signals

Network segmentation takes the concept of offline investigation work looking at bad actor networks and brings it online. Threat investigators, working for a given platform, have the ability to investigate in and around the activities of a known bad actor on their platform and map out the relations and proximity of that bad actor to other online users. Instead of relying on a whack-a-mole approach of removing one-off pieces of content or profiles, network analysis can identify and remove a bad actor network all at once, making it more difficult for that network to rebuild on the platform (Keller et al 2010, Fellman et al 2008). While the account removals aim to get at the known and solidly identified bad actors, what is left can also be a rim of accounts and profiles that had engaged with and been associated with the network, but didn’t meet the threshold for removal based on whatever the criteria of the platform was. This group is both vulnerable and at-risk and makes a key segmented audience for positive interventions and redirections for support. These audiences are lower prevalence, but higher risk, compared with one-off content signal users, having been more concretely identified for the relation to a TVE network.

The content, behaviors, and network signals can thus help guide the formation of refined segmented audiences online to target with positive intervention treatments. Signals can also help inform how much the online user might be upstream or downstream on a radicalization pathway. The more segmentation and layered threat detection can be deployed, the more nuanced a positive intervention strategy can connect the right intervention with the right audience to assist in effective impact (Thorley & Saltman 2023, Brynielsson et al 2012, Cohen et al 2014, Scrivens et al 2017). Much has been progressed in the last 15 years to inform effective interventions. Treatments where the message, messenger, and platform are aligned to the likes, interests, and behaviors of the intended online audience have more chance for impact (Saltman & Zamir 2024). The Radicalisation Awareness Network (RAN) developed the

GAMMA methodology that guides positive interventions to think through the intended goal, audience, messenger, medium, and call to action in order to successfully develop and deploy interventions (Rosata 2021). What success looks like should also be dictated by the ultimate goal, identified audience, and measurement against the call to action.

In the best-case scenario, content, behavioral, and network indicators facilitate audience segmentation at scale, while human oversight adds nuance and quality control to the process (van der Vegt et. al 2019, Thorley & Saltman 2023). In the worst-case scenario, processes could yield high false/positives or false/negatives, leading to erroneous audience segmentation that could have negative effects on the targeted youth users. The next section reviews leading positive intervention tactics led in-house by platforms as well as in partnership with external partners that serve as credible messengers.

Platform Intervention tactics & Partnership Models

Depending on the severity of the signal, a platform might decide to remove a profile and even report it to relevant law enforcement where appropriate if the cases involve credible threat or have links to child exploitation. However, in many cases the signal segmenting an audience can help inform appropriate counter measures and interventions such as; adding friction to an online user journey, creating an educational moment for the user, surfacing counter-content, or providing an alternative pathway for engagement. This section reviews five positive intervention methodologies:

1. Ads Targeting
2. Search-based Redirect Method
3. Violation-based Content Surfacing
4. Strategic Network Disruptions
5. AI Chatbot Deradicalization/Disengagement

Each tactic differs in terms of the human resources, advanced tooling, and partnership model needed to deploy effectively and accurately. Each method also varies in terms of whether or not the intended consequence is a behavioral or sentimental change in the targeted audience. These factors, in turn, can have a large effect on a platform's ability to develop out the capacities needed for launching a given programmatic effort.

	Technical Tooling	Human Resource	Partnership
Ads Targeting	Both in-built and bespoke ads targeting tools can be used. NGO practitioners can deploy ads without formal platform partnerships.	An NGO running an ad targeting campaign without platform partnership only needs their staff management and oversight.	A platform could run their own in-house developed messaging, or an NGO could run their own ads targeted campaign. Partnered models allow scale and nuanced data.
Search Redirect	Once a Redirect Method pipeline has been set up on a platform, subsequent models and redirect pathways are easier to set up.	Significant human oversight is needed from expert/NGO partners to develop key terms lists in partnership with the platform and in the first week of launch a lot of platform and NGO oversight is needed.	Partnerships are critical to understand the terrorist and violent extremist threat phrases and keywords. Partnerships are also often needed as being the end point for where Redirections take a user.
Violation-Based Content Surfacing	The tooling needs are twofold, to ensure a pipeline of users relating to specific violations is set up, and then a rate/frequency pipeline of predesignated content to serve that pipeline needs to be applied.	In its initial set up, high human resource from an NGO to develop content might be needed and in the first weeks of deployment a platform should have a data scientist monitor results.	Programs and partnership management is needed to develop the content for platform deployment.

	Technical Tooling	Human Resource	Partnership
Strategic Network Disruptions	Tooling is needed to help identify harmful network trends as well as pipelines to deploy the disruption and related content to users post-disruption.	Threat investigation teams work closely with the tooling to identify the network. Product policy and data scientists are also needed in the disruption phase.	This can be done completely internally to a platform. Initial threat detection trends could come from law enforcement or third parties. SND content to remaining users could be developed by a partner.
AI Chatbot Disengagement Support	Significant bespoke chatbot product development is needed.	App developers, psychologists working with extremist offenders, and user researchers are all needed.	In early models this has been deployed in partnership with an expert NGO, tech developers, prison reform programs, and psychologists.

Figure 2. Resource Needs and Corresponding Positive Intervention Options

Ads Targeting

Ads-based targeting to deploy alternative and counter-narratives is one of the most known and researched methods for NGOs and civil society groups looking to launch positive interventions online. This method was popularized in the 2010s with hundreds of activists, NGOs, and CSOs working both independently and in partnership with leading social media platforms to have their counterspeech campaigns reach their target audiences via ads-marketing tools. This peaked as global alignment on countering DAESH recruitment of online audiences saw government, tech, and civil society acting against an agreed enemy. Ads tools can facilitate the targeting of audiences with creator content based on likes, interests, and behaviors that are tracked by a given platform. In essence, the same tools used on a platform by private companies to sell younger audiences a particular brand of shoe in a given country, can be re-appropriated to target audiences with psychosocial alternative- and counter-narratives to prevent and counter violent extremism. YouTube's Creators for Change across Asia and abroad (see UNDP Overview) and Meta's Online Civil Courage

Initiative in Europe in partnership with ISD Global (see ISD OCCI Overview). are two examples where leading social media companies built international CSO training programs to upskill civil society practitioners on how to develop, launch, and measure the effectiveness of counter-narrative campaign content through ads targeting, often giving participants free ad grants.

The tooling needed to deploy ads-targeted content is relatively straightforward on most major social media platforms and can be utilized with or without a formal partnership between an NGO and platform. However, the content being deployed is primarily civil society content - not the voice of the platform - to facilitate credible messengers and messages. In the cases of deeper tech-NGO partnership models, greater access to refined audience segmentation and metrics used for success go a long way. Human oversight by the NGO is needed for this work to be effective. Human oversight ideally tracks the engagement on the deployed content to measure its effectiveness. For example, if an NGO uses ads tools to target young audiences with a one minute video, the metrics provided by the ads tooling can show anonymized data on; the average age the ad is reaching traction with, at what point in the video most viewers dropped out, like count, shares of the content, comments on the content, and gender distribution of male/female audiences. Depending on the platform, it can also usually show how much the content reached its target audience purely through the funded ad placement, in comparison to its "organic reach", whereby audiences began to share the content outside of the ads targeting. These metrics can all be used to quickly assess the effectiveness of an online campaign, allowing the creator of the content to edit the content to be more effective as it evolves, or engage with the audiences that have liked and commented on the content - turning passive content surfacing into active engagement.

Search Redirect

In comparison to the ads targeting approach, search redirection is only accessible for an NGO or government if they have a formal partnership with the platform in question. For online interventions aimed at preventing youth radicalization, this form of intervention happens based on an identified list of keywords, phrases or terms of concern (see: European Commission 2022). The list will normally relate to known queries used to seek out terrorist and violent extremist groups, activities, content, or individuals. When a user queries a search function in a way that relates to this list, a pre-developed message about the harmful nature of the query surfaces up top of results, or a pre-determined set of non-harmful alternative or intervention results surface as the top results. This methodology was first developed by Jigsaw, an incubator within Google that aims to build social-good technologies, in partnership with Moonshot. Originally launched for Google Search and YouTube Search functions, this has subsequently been developed and deployed by Facebook, Instagram, and Bing.

The Redirect Method can be programmed to lead users towards factual, educational, or counter-content in aid of creating resilience against radicalization. Measuring click-through-rates (CTR) and engagement on the links provided can assess basic engagement and effectiveness (Helmus & Klein 2018). However, some companies, such as Meta, have developed Search Redirect to facilitate putting the user in touch with local organizations that sensitively disengage individuals away from specific violent extremist organizations (Osman 2022). In these cases, nuanced partnership models are needed and metrics for success can include the ability of the 3rd party "exit program" to assess sentiment analysis on participants who engage with their surfaces after the redirection.

From a technical stance, the redirection needs to be developed by the platform in question. The key term list for words, phrases, or prompts that lead to a redirection treatment alongside the results the redirection surfaces, need to be culturally, linguistically, and geographically relevant to the target audience. Key term lists might also need review and updating as adversarial shifts occur. For these reasons, a good deal of technical support from a platform and human oversight from both the platform and NGO partner are needed, particularly in the initial build and deployment of the intervention model.

Violation-Based Content Surfacing

Violation-based content surfacing is a mechanism whereby when a user shows a hard indicator of engagement with a TVE piece of content, an automated soft response is initiated by serving the user a set amount of relevant counterspeech over a specified period. One of the key ideas behind this methodology was that a one-off intervention of counterspeech content was unlikely to change the sentiment of an online audience, so a series of content over a period of time would be better. This was tested by Facebook based on Stanford University research on content exposure and sentiment change. The study found that to measure a shift in sentiment away from a hate-based belief, the treatment needed to surface 2 to 3 pieces a day of counter or alternative narrative content for between 5 to 7 days (Kirby et. al. 2018). The Facebook treatment using this as a basis for testing showed that a close partnership was needed with the NGOs developing country and language specific counter-narrative content. Once results were filtered for false/positives, the test indicated that true/positive users exposed to the treatment decreased and, in some cases, fully stopped posting and engaging with TVE content thereafter.

The more nuanced and partnered a positive intervention approach, the higher tooling and human resources are needed. This type of treatment has relatively high technical costs, asking that specific violation-based content actions lead to nuanced and time bound content being surfaced to the at-risk user. Many variables can impact the effectiveness of the treatment as well, for example, if the user is not a daily user

of the platform or is based in one country but speaks another language. The methodology also has a high human resource cost for partnership programming needed to develop numerous pieces of intervention content that might be more or less evergreen depending on the TVE violation it relates to.

Strategic Network Disruptions

Strategic Network Disruptions (SNDs) are a method used to disrupt terrorists' and violent extremists' abilities to operate online (Saltman 2020). Similar to offline law enforcement operations tracking bad actor networks, SNDs are significant, targeted actions to remove a dangerous organization's presence online (Lewis 2020). A SND maps a TVE network, including its information exchanges and interrelated signals, in order to remove all verified elements and accounts at once (Keller et al 2010). This tactic has largely been used for removal actions, however, in every SND there is a remaining related group of users left by a targeted action that were associated or familiar with but not fully identified as being part of the network. The profiles of those users are highly vulnerable and at-risk. In recent years, some larger platforms have tested providing those profiles with relevant geographic exit programs to disengage from TVE networks and provide alternative pathways for engagement online with early positive results.

The tooling used to identify TVE entities can be relatively straightforward. However, the human resource needed to carry out SNDs both internally and with potential partnership models is significant. Internal threat investigation teams working with data scientists are needed to identify and refine the relevant segmented audience. Programmatic leads need to identify and work with geographically relevant NGOs or content providers as well. This paper discussed the usage of content, behavior, and network signals to identify at risk and violating profiles of online users. SNDs used for creating a segmented audience bring all three into play when using them to target positive interventions.

AI Chatbot Disengagement Trials

The usage of artificial intelligence (AI) and large language models in online counterterrorism efforts has been evolving for more than a decade. What has shifted in recent years is the rapidly expanding use of AI agents and generative AI (GenAI) by individuals around the world through the accessible uptake of AI optimized search engines, chatbots, and content creation tools. Like most emerging technologies, these powerful tools can lead to harm when deployed by malicious actors, including terrorists and violent extremists, but also have enormous potential in the prevention, positive intervention, and rehabilitation space (Saltman & Gilmore, 2025). Most recently, there have been trials to use controlled chatbots to facilitate rehabilitation therapy of individuals convicted of TVE activities. In the case of Mythos Labs' "Aldous" chatbot,

teams of psychologists are given access to the chatbot information with transparency about data access to the convicted individual, who can opt in to using the chatbot as a psychosocial support tool (see Mythos Labs). Built with Meta's open-source Llama AI system, the chatbot can surface data to the practitioners about the psychological well-being of the user, discourse analysis about grievances, and analysis support on ideological links. Initial results have shown that ~80% of those using the app have opted to continue using it after the trial period (Mathur 2025).

The current reality is that younger audiences are not only using apps and platforms to communicate with friends, learn about the world, and engage in online games but also to find psychosocial support. A US-wide study found that 72% of 11-year-olds owned a smartphone, rising to 84% by age 13 (Life in Media Survey 2025). Many teens are turning to AI chatbots for emotional support, particularly by isolated or minority individuals (Andoh 2025). Some studies have shown that 72% of teens have used AI companions with 12% using them for emotional or mental health support (Robb & Mann 2025). This trend is only set to grow internationally, as GenAI chatbots expand in broad use. For young people in particular, AI chatbots are cheap (often free), are available all hours of the day, don't feel judgmental, and never tire of you. As mentioned previously, positive interventions work well when the message, messenger, and platform are aligned. Meeting young people where they are already at in digital spaces, building in adequate trust and safety engagement programs to support resilience and prevention against TVE ideologies through mechanisms like AI chatbots presents a large opportunity for positive intervention work.

This intervention model is the newest of the listed methodologies and would take serious work before deploying to younger audiences. The tooling is rapidly advancing but would need sensitive large-language models trained in advance with human oversight and parental awareness, among other considerations.

Blockers, Gaps, & Needs

Despite the advanced tooling for segmenting audiences and launching innovative positive interventions to aid in preventing youth radicalization, there remain a number of critical blockers, gaps, and needs for the future of online interventions to be successful. The four primary hindrances are, (1) a lacking international alignment on the threat, (2) a decrease in funding towards PCVE efforts of NGOs and civil society, (3) an increasingly heterogenous online landscape, and (4) ethical and privacy-based sensitivities around targeted youth engagement online.

International Alignment on the Threat

Post 9/11 in the 2000s and at the height of DAESH in the 2010s there was a clear alignment among most government and intergovernmental bodies that Al Qaeda,

DAESH, and all related affiliates were “terrorists”. All praise, support, and representation of these groups, and their affiliates, could be removed online without push-back from national authorities. The United Nations Security Council Consolidated List, where most tech companies find consensus on defining TVE entities, largely consists of organizations and individuals related to these two groups (see: UNSC Consolidated List). Outside of these organizations, there is some alignment when it comes to taking actions against content associated with lone actor attackers. As an example, the GIFCT Incident Response Framework facilitates the quick identification for tech platforms of perpetrator produced content associated with lone actor attacks of a TVE nature, relying on the behavior and nature of the attack to escalate actions. However, outside of these extreme examples of terrorist and violent extremist threats, there is very little global alignment on definitions or designation lists to guide the private sector (See: Global Definitions of Terrorism).

Often, the main concerns around youth vulnerabilities are what some have called “borderline content”, that might not be TVE content but might pose as gateway content or networks leading audiences towards more extreme, hate based ideologies (Saltman & Hunt 2023). Current trends show an increase in non-organizational, decentralized violent extremist networks, particularly aimed at younger audiences online (Comerfield 2020, Davey et al 2021). In parallel, there are also groups that are less ideologically aligned but have clear violent extremist intentions aimed at young online users. Cases of sadistic and nihilist violent extremist incidents whereby perpetrators and victims have been “youth” have increased in recent years (Argentino et al 2024). Incidents of misogyny-based violent extremism has also increased with many educators and parents posing concerns about the mainstreaming of misogynistic content from individuals such as Andrew Tate among young men. None of these trends of violent extremism have government alignment or clear mandates for action to guide tech companies. The more governments can align on definitions, make strong statements about supporting online efforts to counter current TVE trends more broadly, and share knowledge about known bad actor networks, the more tech companies can be assured in taking stronger online actions, without fear of being accused of curtailing free speech.

Civil Society Funding

For many of the mentioned positive intervention strategies, nuanced partnerships between the private and public sector are needed. The credible messengers and expert knowledge about TVE trends in a given country comes mainly from the civil society and academic sector. In recent years the government funding for many CSOs has decreased substantially (Ginkel 2025). In parallel many robust tech company initiatives in partnership with CSOs have also pulled back. Often the signal of funding from the government on key social issues helps drive the impetus for tech companies to put time and effort into similar fields. While the examples given in this

paper of positive interventions show the great potential for partnerships leading to online impact, the scaling up of these partnerships takes significant funding as well as human resource from both government and tech companies. There are also gaps in global implementation of these tactics, since many of the strategic approaches need linguistic, geographical and cultural nuances built into the models (Ogenga 2023). The tools, tactics, and partnership models already exist; however, these won't be able to scale impact and reach without funding and partnership support for key civil society organizations working on youth prevention and resilience.

Heterogenous Platform Landscape

The positive intervention approaches outlined in this paper largely highlight initiatives and models developed by some of the largest tech companies such as Facebook, Instagram, Google Search, YouTube, and TikTok. However, there is a disconnect between these platforms and many other dynamic platforms that younger audiences are engaging with daily. The availability of positive intervention strategies deployed on a wider range of platforms depends on (1) size, (2) in-house expertise, (3) willingness, and (4) platform architecture.

The larger companies, focusing on social media in particular, have the human and tooling resources to deploy nuanced positive intervention models that include partnership funding. They have also faced the most mounting social and governmental pressures to do more in this space. Smaller and medium companies are poorer resourced both in terms of engineering support to build out the pipelines needed for these methodologies, but also having the in-house expert teams to understand the threat fully and be able to engage partners to build out these programmatic efforts. Smaller and medium companies can lean into existing methods, learning from larger companies and using open-source tools where available, however, there still needs to be a dedicated in-house team managing the work. There is also a big question of willingness. There are many smaller, less-regulated platforms that have large youth user bases but do not have an open-door to partnerships - be it with civil society organizations or other tech platforms. These are often semi or fully encrypted chat platforms or novel gaming platforms that take a robust "free speech" approach and lean away from scaled moderation or intervention more broadly.

Lastly, there are a range of platforms that younger audiences are highly engaged on but that have a different architecture and user experience so that positive intervention methodologies would have to be re-conceptualized to fit these spaces. This includes gaming and gaming adjacent platforms as well as marketplace/e-commerce sites, audio-based platforms, and nouveau social media sites with short form video formats. These platforms will be key in the future for alternative intervention strategies, meeting young audiences where they are most engaged.

Sensitivities for Youth Engagement

There are a range of sensitivities that need to be considered when developing online interventions aimed at preventing youth radicalization. The concepts around defining and segmenting audiences based on terrorist and extremist based signals can be controversial. Indicators used to target “extremism” can be easily politicized by social and political groups. Adding the layer of “youth” as a key segmented audience can also be controversial. Broad education about digital literacy is one thing but engaging young people on topics about hate based extremism needs extra layers of sensitivity when the audience is under 18. Within that segmentation, there is a large difference between the material that might be adequate to engage a 17-year-old, versus a 13-year-old or younger, depending on the platform age restrictions. This is further strained by an increasing disconnect between the social norms and spaces used by youth users in comparison to parent or teacher users. The language and online behaviors of young people, as well as the platforms they engage on, vary drastically from older generations. That disconnect is another factor that makes it increasingly difficult to bring parents and teachers into prevention and resilience strategies.

Preventing and countering hate-based extremism among young online audiences needs a new wave of ethical and human rights reviews, in consultation with parents, educators, and government to decide how best to deploy positive interventions to reach young users. While there are not clearly agreed steps all platforms should take for assessing algorithmic tools or intervention practices, some international bodies have progressed on guidance. Aimed at industry policies and practices, the UNHR's Guiding Principles on Business and Human Rights is a bedrock for tech companies (see: UNHC Guiding Principles 2011).

Conclusions & Next Steps

As shown, there is already an advanced understanding of TVE related harms online through the review of content, behavioral, and network signals. There are also already a range of methods using these signals to facilitate audience segmentation for launching nuanced positive interventions. The tactics, tools and insights all exist to advance youth-focused prevention against radicalization towards hate-based extremism. Some of these tactics could engage young audiences through pathways that lead to offline resources, while others might provide AI-facilitated psychosocial support in the future. A key issue is that the scaled deployment of these tactics is currently missing, with the main innovation still taking place on only a few of the largest tech platforms, with unequal geographic distribution in partnerships and programs.

However, the pieces exist to further positive intervention work if governments, the private sector, and civil society have the right infrastructure and funding to work

together. Spaces for a diversity of tech companies to share lessons learned will continue to be critical. Knowledge-exchange between government and tech companies to discuss the online-offline threat landscape are key to developing awareness and understanding the signals indicating threats towards young online audiences. It will also be important for governments to articulate their support for youth prevention work, including the funding support towards civil society groups working on youth safety issues. Networks that facilitate this all-of-society approach should be grown, whether that is the Global Internet Forum to Counter Terrorism working directly with a range of tech platforms, the EU Internet Forum bringing platform awareness to policy makers, the Aqaba Process convening diverse geographical intelligence bodies with technical awareness, or various UN initiatives.

References

(2021). *Content-Sharing Algorithms, Processes, and Positive Interventions Working Group: Positive Interventions*. Global Internet Forum to Counter Terrorism. July. See: <https://gifct.org/wp-content/uploads/2021/07/GIFCT-CAPI2-2021.pdf>.

(2024). "Young people and violent extremism: a call for collective action". *Five Eyes Insights*. See: <https://www.nzsis.govt.nz/assets/NZSIS-Documents/Young-People-and-violent-extremism-a-call-for-collective-action.pdf>.

(2024). "Number of young people arrested for terrorism offences hits record high". *Counter Terrorism Policing*, 15 March. See: <https://www.counterterrorism.police.uk/number-of-young-people-arrested-for-terrorism-offences-hits-record-high/>.

(2025). *2025 Life in Media Survey: A Baseline Study of Digital Media Use and Well-being Among 11- to 13-year-olds.* University of South Florida. See: <https://www.usf.edu/arts-sciences/departments/journalism/documents/lims2025/lims2025.pdf>.

Andoh, Efua. (2025). "Many teens are turning to AI chatbots for friendship and emotional support", *American Psychologist Association.* Vol.56., No.7. (1 October). See: <https://www.apa.org/monitor/2025/10/technology-youth-friendships>.

Argentino, Marc-André; G. Barrett, M.B. Tyler. (2024). "764: The Intersection of Terrorism, Violent Extremism, and Child Sexual Exploitation". *GNET Insight Series.* See: <https://gnet-research.org/2024/01/19/764-the-intersection-of-terrorism-violent-extremism-and-child-sexual-exploitation/>.

Bell, Stewart and David Akin. (2025). "In briefing to minister, RCMP warns of 488% jump in terrorism charges". *Global News Canada*. 23 May. See: <https://globalnews.ca/news/11194439/briefing-minister-rcmp-jump-in-terrorism-charges/>.

Braddock, Kurt. 2020. Weaponized Words. Cambridge: Cambridge University Press.

Brynielsson, Joel; Andreas Horndahl, Fredrik Johansson, Lisa Kaati, Christian Mårtenson and Pontus Svenson, “Analysis of Weak Signals for Detecting Lone Wolf Terrorists” (2012 European Intelligence and Security Informatics Conference, 2012), 197–204, doi: 10.1109/EISIC.2012.20.

Comerfield, Milo. (2020). “Confronting the Challenge of 'Post-Organisational' Extremism“. *Raisina Debates Essay Series.* Observer Research Foundation. (19 August). See: <https://www.orfonline.org/expert-speak/confronting-the-challenge-of-post-organisational-extremism>.

Cohen, Katie; Fredrik Johansson, Lisa Kaati and Jonas Clausen Mork, “Detecting Linguistic Markers for Radical Violence in Social Media,” *Terrorism and Political Violence* 26, no.1 (2014): 246–56, DOI: 10.1080/09546553.2014.849948.

Davey, Jacob; Milo Comerford, Jakob Guhl, Will Baldet, Chloe Colliver. (2021). *A Taxonomy for the Classification of Post-Organisational Violent Extremist & Terrorist Content*. ISD Global. See: <https://www.isdglobal.org/wp-content/uploads/2022/01/A-taxonomy-for-the-classification-of-post-organisational-terrorist-content.pdf>.

European Commission. (2022). *The Redirect Method (TRM)*. European Commission: Migration and Home Affairs. See: <https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/redirect-method-trm_en>.

European Parliament. (2025). “Terrorism in the EU: trends, terror attacks and arrests in 2023”. *European Parliament Topics.* 1 January. See: <https://www.europarl.europa.eu/topics/en/article/20250124STO26468/terrorism-in-the-eu-trends-terror-attacks-and-arrests-in-2023>.

Fellman, Philip V., Jonathan P. Clemens, Roxana Wright, Jonathan Vos Post, and Matthew Dadmun, “Disrupting Terrorist Networks, a Dynamic Fitness Landscape Approach,” *ArXiv:0707.4036 [Nlin]*, 2008, http://arxiv.org/abs/0707.4036.

GIFCT. (2025). *2024 GIFCT Annual and Transparency Report*. Global Internet Forum to Counter Terrorism. See: <https://gifct.org/wp-content/uploads/2025/07/GIFCT-Annual-and-Transparency-Report-2024.pdf>.

GIFCT. (2023). *Playbook on Positive Intervention Strategies Online: GIFCT Blue Team Working Group.* Global Internet Forum to Counter Terrorism. See: <https://gifct.org/wp-content/uploads/2023/11/GIFCT-23WG-1023-Playbook-1.1.pdf>.

Ginkel, Bibi van. (2025). *Under Pressure: Rethinking Comprehensive Approaches to CT and P/CVE in an Age of Austerity and Instability*. ICCT Policy Brief. 3 September. See: <https://icct.nl/publication/under-pressure-rethinking-comprehensive-approaches-ct-and-pcve-age-austerity-and>.

Global Definitions of Terrorism. (n.a.). *The Definitions & Principles Framework Project*. Global Internet Forum to Counter Terrorism.

See: <https://def-frameworks.gifct.org/global-definitions-of-terrorism/>.

Helmus, Todd and Kurt Klein. (2018). *Assessing Outcomes of Online Campaigns Countering Violent Extremism: A Case Study of the Redirect Method.* RAND Corporation. <https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2813/RAND_RR2813.pdf>.

ISD Global. (n.a.). *The Online Civil Courage Initiative (OCCI)*. ISD Global. See: <https://www.isdglobal.org/isd-programmes/online-civil-courage-initiative-occi/>.

Keller, Jared; Kevin C. Desouza, and Yuan Lin, "Dismantling Terrorist Networks: Evaluating Strategic Options Using Agent-Based Modeling," *Technological Forecasting and Social Change* 77, no.7 (2010): 1014–36. See: <https://doi.org/10.1016/j.techfore.2010.02.007>.

Kirby, Leo; Margaret Williams, and Jorge Ramirez Mata. (2018). "Counterspeech: How Does Online Counterspeech Impact Real World Behavior?," *IPS Practicum MA Project.* Stanford University.

Kowert, Rachel and Sarah Chittick. (2025). *Threat Surfaces in Games: Challenges and Best Practices*. Year 4 Working Groups. Global Internet Forum to Counter Terrorism. See: <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-Threat-Surfaces-1.1.pdf>.

Lamphere-Englund, Galen. (2025). *Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces*. Year Four Working Groups. Global Internet Forum to Counter Terrorism. See: <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-PDR-Surfaces-1.1.pdf>.

Lewis, Jonathan. (2020). "Facebook's Disruption of the Boogaloo Network," *GNET Insight*. See: <https://gnet-research.org/2020/08/05/facebooks-disruption-of-the-boogaloo-network/>.

Mathur, Priyank. (2025). "[Presentation on Panel Two] Collaborative Interventions: Countering New Threats With Cross-Sector Solutions". *Rewriting the Playbook: Online Subcultures, Child Exploitation, and the Shifting Landscape of Terrorism*. UNGA Side Event hosted by the Global Internet Forum to Counter Terrorism. 24 September.

Mythos Labs. (n.a.). *AI Solutions*. See: <https://mythoslabs.org/ai-solutions/>.

Ogenga, Fredrick. (2023). "Strategizing Online Interventions in Global Contexts". *Playbook on Positive Intervention Strategies Online: GIFCT Blue Team Working Group.* Global Internet Forum to Counter Terrorism. See: <https://gifct.org/wp-content/uploads/2023/11/GIFCT-23WG-1023-Playbook-1.1.pdf>.

Osman, Nawab. (2022). *Expanding Counterspeech Initiatives Into Pakistan and the UK.* Meta Blog. 9 February.

<https://about.fb.com/news/2022/02/facebook-counterspeech-in-pakistan-uk/>.

Robb, M.B., & Mann, S. (2025). *Talk, trust, and trade-offs: How and why teens use AI companions*. Common Sense Media. See:

<https://www.commonsensemedia.org/sites/default/files/research/report/talk-trust-and-trade-offs_2025_web.pdf>.

Rosata, Valeria. (2021). “Evaluating the Effectiveness of Online Counter-Messaging Campaigns Against Radicalisation and Violent Extremism”. *Rivista Trimestrale di Scienza dell’Amministrazione: Studi di teori e ricerca sociale*. 4/2021. See: <https://rtsa.eu/RTSA_4_2021_Rosato.pdf>.

Saltman, Erin. “Countering Terrorism and Violent Extremism at Facebook: Technology, Expertise and Partnerships.” *Global Policy - Observer Research Foundation Series: Tackling Insurgent Ideologies in a Pandemic World*. (August 2020): Chapter 14, 80 – 85. https://www.orfonline.org/expert-speak/countering-terrorism-and-violent-extremism-at-facebook/

Saltman, Erin and Micalie Hunt. "Borderline Content: Understanding the Gray Zone." *Global Internet Forum to Counter Terrorism.* 2023. *Originally a published contribution to the European Union Internet Forum (EUIF) handbook on Borderline Content. Published for Open Access by GIFCT. https://gifct.org/wp-content/uploads/2023/06/GIFCT-23WG-Borderline-1.1.pdf

Saltman, Erin, Farshad Kooti & Karly Vockery. “New Models for Deploying Counterspeech: Measuring Behavioral Change and Sentiment Analysis.” *Studies in Conflict & Terrorism*. 2021. https://www.tandfonline.com/doi/full/10.1080/1057610X.2021.1888404

Saltman, Erin and Munir Zamir. "Chapter 8: The Future of Counterspeech : Effective Framing, Targeting, and Evaluation." in *Counterspeech : Multidisciplinary Perspectives on Countering Dangerous Speech*, edited by Stefanie Ullman and Marcus Tomalin. Oxon : Routledge, 2024.

Scrivens, Ryan; Garth Davies, and Richard Frank, “Searching for Signs of Extremism on the Web: An Introduction to Sentiment-based Identification of Radical Authors,” *Behavioral Sciences of Terrorism and Political Aggression* 10 (2017): 1–21.

Thorley, Tom and Erin Saltman. "GIFCT Tech Trials: Combining Behavioural Signals to Surface Terrorist and Violent Extremist Content Online." *Studies in Conflict & Terrorism*. 2023. https://www.tandfonline.com/doi/full/10.1080/1057610X.2023.2222901

UNDP. (n.a.). “YouTube Creators for Change”. *Asia and the Pacific*. UNDP Overview. See. <https://www.undp.org/asia-pacific/youtube-creators-change>.

United Nations Human Rights, Office of the High Commission, (2011). *Guiding Principles on Business and Human Rights*. OHCHR. See: <https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

UNODC. (2017). *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*. UN Office of Drugs and Crimes. See: <https://www.unodc.org/documents/justice-and-prison-reform/Child-

Victims/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf>.

UNSC. (n.a.). *United Nations Security Council Consolidated List*. See: <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>.

van der Vegt, Isabelle; Paul Gill, Stuart MacDonald, and Bennett Kleinberg. (2019) "Shedding Light on Terrorist and Extremist Content Removal," Royal United Services Institute. See: <https://rusi.org/explore-our-research/publications/special-resources/shedding-light-on-terrorist-and-extremist-content-removal>.

Zamir, Munir. (2022). *Active Strategic Communications: Measuring Impact and Audience Engagement : GIFCT Positive Interventions and Strategic Communications Working Group*. Global Internet Forum to Counter Terrorism. See: <https://gifct.org/wp-content/uploads/2022/07/GIFCT-22WG-PI-Impact-1.1.pdf>.

CHAPTER 10

Strategic Foresight and Counter-Terrorism Futures: Aligning NATO Doctrine with Emerging Threats and Structural Drivers

Dr. Gergely Németh

Abstract

This chapter examines the future trajectory of counter-terrorism through the lens of NATO's existing doctrinal frameworks and strategic foresight analysis.[5] By establishing a baseline with the Strategic Concept 2022, Allied Joint Publication-01 (AJP-01), NATO's 2024 Policy Guidelines on Counter-Terrorism, and the Defence Against Terrorism Centre of Excellence's institutional roles, responsibilities and contributions, this analysis extrapolates critical challenges and opportunities against the futures assessment of Strategic Foresight Analysis 2023.

The research emphasizes that emerging disruptive technologies, climate breakdown, resource scarcity and empowered human networks will fundamentally transform the character of terrorism and consequently, Allied responses. The pervasive competition scenario emerges as most probable, requiring NATO to adapt its counter-terrorism posture toward integrated, multi-domain operations addressing cognitive, virtual, and physical dimensions simultaneously.

The chapter concludes that gaps exist in current doctrine (AJP 0.1) regarding non-state actor empowerment, technological governance, climate-security nexus integration, and hybrid warfare-terrorism convergence.

NATO's institutional response provides a necessary foundation for transformation but at the same time, efforts to provide deeper doctrinal analysis and strategic policy evolution will be necessary to successfully counter the emerging tenets of future terrorism. Futures thinking will provide great value to this effort.

[5] As of 2025.

1. Introduction

The contemporary security environment represents a paradigmatic shift in the nature and scope of threats confronting the North Atlantic Alliance. Since NATO's Article 5 invocation following 11 September 2001, which constituted the sole activation in Alliance history, counter-terrorism has evolved from a peripheral concern to a core strategic priority spanning across NATO's defence and deterrence architecture (Hallams, Ratti, and Zyla, 2013; Sandler, 2015; Pomarede, 2024).

The 2022 Strategic Concept already explicitly identified terrorism as “the most direct asymmetric threat to the security of NATO citizens and to international peace and prosperity,” establishing the baseline from which contemporary threat assessments depart. At the same time, terrorism is still undergoing fundamental transformation, driven by the emerging global security environment. This environment could be understood as a complex system, and as such, its attributes are also in constant flux. Such dynamics can also be understood as a causal relation between the system and structural forces which are driving its emergent behavior, attributes and traits (Alberts and Czerwinski, 1997; Jervis 1997). The relevant structural forces (drivers) have first been identified by the analytic community of the North Atlantic Treaty Organization as part of the NATO Strategic Foresight Analysis research project in 2022-2023. The SFA23 identified these structural drivers as agents of change, forming a shift of a more benign security environment into an age of “pervasive competition” characterized by complexity, congestion, commercialization, contestation, and confusion extending through the decade to 2043 (NATO Allied Command Transformation, 2023).

This chapter aims to address long-term trajectories, opportunities and challenges for Allied counter terrorism efforts. In order to do so, it employs a scenario-based methodology anchored in NATO's foresight architecture to explore counter-terrorism futures in three distinct pathways (NATO SFA, 2023).

The research design integrates doctrinal tenets (as showcased in NATO`s Allied Joint Publication 0.1), with the 2024 Policy Guidelines' three operational pillars of awareness, capabilities, and engagement. Against this baseline, SFA23's seven drivers of change provide the analytical framework for understanding how climate breakdown, resource scarcity, emerging disruptive technologies, geoeconomics, human networks, the scramble for commons, and international order transition will reshape terrorist threat environments. This analysis also incorporates the institutional role of NATO's Defence Against Terrorism Centre of Excellence (DAT COE).

The research question addresses a fundamental challenge facing NATO's strategic community: *how will these evolving qualities challenge and enable current*

counter-terrorism thinking, guidelines, and actions across plausible future pathways to 2043?

2. Foundational Frameworks: Doctrine, Policy, and Institutional Enablers

2.1 Allied Joint Doctrine: The Conceptual Architecture

AJP-01 establishes the intellectual foundation for NATO's military instrument of power through four key tenets (the behaviour-centric approach, the manoeuvrist approach, the comprehensive approach, and mission command) that directly inform counter-terrorism operations. The behaviour-centric approach recognizes that terrorist organizations target audiences far beyond immediate victims, seeking systematically to manipulate public perception, erode institutional trust, and polarize societies. This approach partitions audiences into public, stakeholders, and actors. These categories are particularly relevant when assessing how terrorist networks exploit social media and human networks to achieve recruitment at scale. The manoeuvrist approach, pitting strength against vulnerability, becomes increasingly critical as terrorist actors employ asymmetric tactics across multiple domains simultaneously, from cyberspace to cognitive space to the physical realm. The comprehensive approach combines political, military, and civilian capabilities and addresses the reality that counter-terrorism “remains primarily with national civilian and legal authorities” while NATO's role is complementary and non-duplicative (NATO Washington Summit, 2024). This principle underlines that military force alone cannot defeat terrorism and enduring success requires orchestrating effects across diplomatic, information, economic, and military instruments of power. Mission command, with its emphasis on centralized intent and decentralized execution, enables rapid adaptation essential for responding to terrorist threats that operate at accelerated decision cycles, often faster than traditional military planning processes.

AJP-01's conflict triangle (contradiction, attitude, and behaviour) also provides utility for better understanding terrorist radicalization pathways. Contradictions (grievances, ideological disputes) shape attitudes (hostile perceptions toward state institutions or Western powers) that manifest in violent behaviour. This framework illuminates how climate breakdown and resource scarcity create new contradictions that terrorist actors actively exploit and amplify, while emerging technologies amplify actors' ability to shape attitudes and coordinate behaviour at previously unimaginable scale and speed.

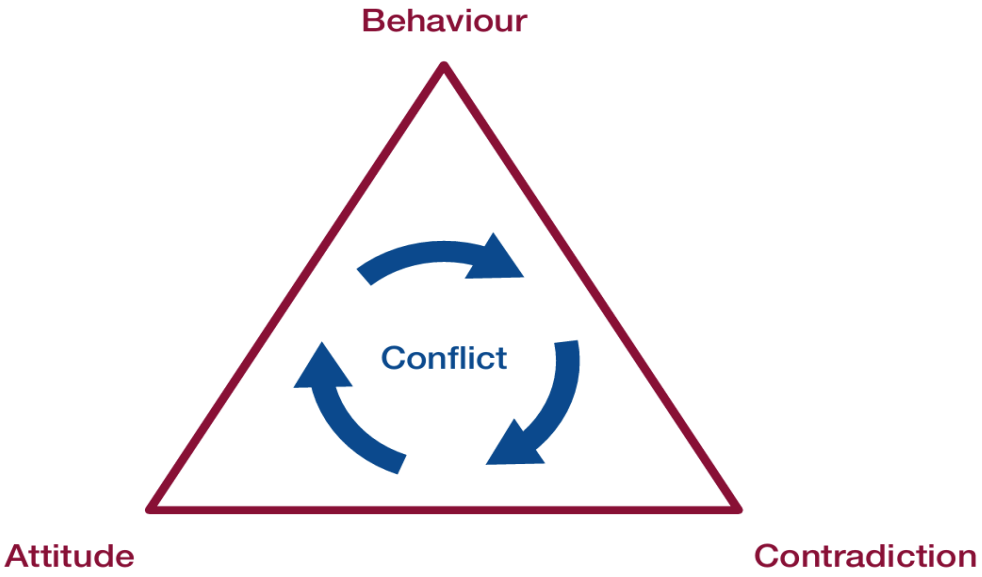


Figure 3: The conflict triangle. Source: Allied Joint Publications 0.1 (NATO Standardization Office 2022)

In the context of NATO's efforts to frame the complexity of contemporary security challenges, including terrorism, AJP-01's true utility lies in providing an analytical lens through which NATO's dedicated counter-terrorism policy can be interconnected with other analytical efforts, such as long-term strategic foresight. The conflict triangle connects structural drivers and grievances to observable attitudes and behaviours, providing a bridge between strategic foresight on climate, technology or governance trends and the practical design of awareness, capability and engagement measures. Against this backdrop, the 2024 Counter-Terrorism Policy Guidelines can be understood as the operationalisation of AJP-01's logic: they translate the conceptual architecture, and the conflict triangle's emphasis on contradictions, attitudes and behaviours, into concrete lines of effort, institutional arrangements and partnerships that underpin NATO's evolving counter-terrorism posture.

2.2 NATO's 2024 Counter-Terrorism Policy Guidelines: Strategic Evolution

The updated Policy Guidelines, endorsed at the 2024 Washington Summit, reflect a decade of operational learning and strategic adaptation. The document organizes counter-terrorism efforts around three core areas: improving threat awareness through enhanced intelligence sharing and strategic analysis, ensuring adequate capabilities and preparedness through doctrine and capability development, and enhancing engagement with partners and international organizations through sustained dialogue and capacity-building. Three foundational principles govern these efforts: compliance with international law and human rights frameworks, support to Allies in collective defense, and non-duplication with complementary mandates of the UN and other international organizations.

The Guidelines explicitly recognize terrorism's evolving character, noting that terrorists “continue to commit or inspire horrendous attacks, and undermine security in Allies' own territory” (NATO Washington Summit, 2024, p. 7). The Guidelines also emphasize resilience-building, reflecting lessons from hybrid warfare that terrorist actors often seek to exploit societal vulnerabilities and critical infrastructure interdependencies. Critically, the Guidelines establish the Secretary General's Special Coordinator for Counter-Terrorism as the institutional focal point, signalling NATO's commitment to sustained strategic focus and elevating counter-terrorism to the highest levels of Alliance decision-making (NATO Washington Summit, 2024; Pomarede, 2024).

2.3 NATO Defence Against Terrorism Centre of Excellence: Institutional Hub and Transformation Catalyst

The Defence Against Terrorism Centre of Excellence (DAT COE) in Ankara, Türkiye, transforms NATO's doctrinal tenets and policy guidelines into tangible capabilities, within its education and training opportunities, and serves as the Alliance's primary institutional hub for counter-terrorism expertise. Established in 2005 with seven NATO member nations, COE-DAT occupies a unique position outside the NATO Command Structure, enabling independent transformation efforts while maintaining functional alignment with Allied Command Transformation.

DAT COE executes its mission through four primary functions: education and training, research and analysis, concept development, and lessons learned management. To date, the center has conducted 328 activities in 22 countries, including 39 mobile training programs, with 3,505 trainers and 14,942 trainees from 124 countries, totaling 18,447 participants .[6] The Centre directly implements the 2024 Policy Guidelines' three pillars by conducting horizon-scanning research on emerging trends, developing specialized courses on critical infrastructure protection and weapons of mass destruction, and hosting annual conferences that convene practitioners from over 35 countries. Recent research volumes on "Climate Change and Terrorism" and "The Weaponization of Artificial Intelligence" demonstrate the Centre's capacity to anticipate how SFA23's drivers transform terrorist methodologies.

The Centre's 2025 workshop agenda underscores its strategic focus on emerging threats, including adapting NATO Counter-Terrorism Approach in a Multi-Domain Operational Context, which operationalizes AJP-01's multi-domain operations concept across physical, virtual, and cognitive dimensions.

[6] NATO counterterrorism center in Türkiye bolsters global security efforts - Türkiye News. Accessed: 10 May, 2026

3. The Security Environment Transformation: SFA23's Seven Drivers and Implications

3.1 Why SFA23 Matters: Understanding Systemic Security Change

SFA23 is NATO's most comprehensive futures research since 2017. It provides an essential baseline for understanding transformative security environment change through 2043. Its critical importance stems from three functions that address fundamental challenges in strategic planning under deep uncertainty. First, it creates shared understanding across Allies and Partners by aligning disparate national foresight efforts around common drivers and scenarios. This is highly essential because, as the analysis acknowledges, “the futures thinking of various nations and stakeholders within the Alliance do not align by default” (NATO Allied Command Transformation, 2023, p. 11). Without this shared framework, Allied defence planning fragments into 31 separate threat assessments, undermining interoperability and efficient resource allocation. The report's deliberately bleak and risk-focused approach served as a wake-up call for planners that emerging disruptions and changes have to be taken into account across all military planning assumptions (NATO Allied Command Transformation, 2023).

SFA23 has updated older assumptions from previous analyses highlighting new, systemic shocks that have “gravely altered” the security environment (NATO Allied Command Transformation, 2023, p. 12). COVID-19 and Russia's full-scale invasion of Ukraine demonstrated that linear projections collapse under cascading, interconnected crises. These shocks revealed how disruptions in one domain (public health, territorial sovereignty) cascade across economic, technological, and social systems, creating novel threat vectors that traditional planning failed to anticipate (Rainero & Tagarev, 2024). SFA23's methodology addresses this non-linearity through the Framework Foresight Model, emphasizing “sense-making under conditions of deep uncertainty rather than probability-based prediction” (Hillebrand, 2022, p. 19).

The report also translates geopolitical trends into concrete military implications. By identifying how climate constrains force generation, AI transforms operational tempo, and resource scarcity redirects defence spending, SFA23 enables proactive defence planning rather than reactive adjustment to unforeseen crises (NATO Allied Command Transformation, 2023; RUSI, 2024).

SFA23’s findings provide an essential addition to understanding how terrorism may change in practice and in the long-term. This includes how grievances form, how recruitment and radicalization unfold, and how terrorist methods adapt across physical, virtual, and cognitive spaces. Therefore, the next sub-chapters will aspire to show how each driver climate breakdown, new technologies, empowered human networks, the global commons, and a fragmenting international order reshapes

opportunities, constraints, and behaviours of terrorist actors, thereby linking systemic change to the concrete evolution of terrorism.

3.2 Context: A Security Environment in Structural Disruption

SFA23's analytical baseline is the “fragmenting world” established in NATO's 2022 Strategic Concept. This environment is defined by interlocking crises: Russia's violation of Ukraine's sovereignty represents the gravest rules-based international order (RBIO) challenge in Europe since World War II, demonstrating how 21st-century conflict combines kinetic operations with critical infrastructure attacks, information warfare, and economic coercion. These are also tactics that terrorist actors observe and actively emulate (Shentov & Petrov, 2024).

A “polycrisis” dynamic is omnipresent in the findings, meaning that climate-induced migration, resource scarcity, and technological disruption amplify each other rather than occurring in isolation, creating increasingly frequent structural disruptions (Rainero & Tagarev, 2024; Quillian & Campbell, 2025). The “Fourth Industrial Revolution” compresses technology development cycles, democratizing capabilities once reserved for states while governance gaps create spaces for terrorist exploitation (NATO Allied Command Transformation, 2023). Urbanization and technology-enabled human networks create “networked non-state actors” operating more efficiently than traditional institutions in some domains, while “declining trust in governments” fuels radicalisation in congested information environments (NATO Allied Command Transformation, 2023).

Furthermore, the “commercialized” and “congested” attributes of this environment fundamentally alter the terrorism capability calculus. As noted by Schori Liang (2023), the widespread availability of dual-use commercial technologies, from advanced encryption to unmanned aerial systems, grants terrorist actors “state-like lethality” without the requisite industrial base. This commercialization creates a persistent asymmetry where non-state actors can rapidly acquire and weaponize off-the-shelf innovations faster than bureaucratic state procurement cycles can develop countermeasures. Simultaneously, the “congested” information environment allows terrorist narratives to compete on equal footing with state communications; in this ecosystem, "truth" is drowned out by the volume of content, enabling extremists to exploit cognitive biases and tailor radicalization messages to specific micro-audiences with unprecedented precision (Parrish et al., 2024).

Finally, the “confused” and “contested” nature of the security landscape erodes the traditional boundaries between peace, war, and law enforcement, creating ideal conditions for hybrid terrorist threats. The ambiguity inherent in this environment complicates attribution and response, as hostile state actors increasingly utilize terrorist proxies or criminal syndicates to conduct operations below the threshold of

armed conflict, thereby maintaining plausible deniability (Shentov & Petrov, 2024). Rainero and Tagarev (2024) argue that this blurring of lines challenges existing counter-terrorism legal frameworks, which were designed for clearer distinctions between combatants and civilians. Consequently, the future counter-terrorism environment will likely be characterized by persistent legal and operational ambiguity, where the identity of the adversary remains deliberately obscured to paralyze decision-making within the Alliance (Sartori & Stefanini, 2022; Hillebrand, 2022).

3.3 Climate Breakdown and Resource Scarcity: The Existential Driver

SFA23 identifies climate breakdown as the “most consequential and, in the long-term, the most likely existential challenge,” one that will prompt “significant changes in attitudes and behaviours of both state and non-state actors” (NATO Allied Command Transformation, 2023, pp. 22–28). For counter-terrorism specifically, this manifests through multiple causal pathways. The Sahel exemplifies this dynamic comprehensively. With temperatures rising around 1.5 times the global average, the region faces cascading pressures: rising temperatures destabilize traditional pastoral and agricultural livelihoods, forcing nomadic populations into competition over shrinking water and grazing resources (Visser & Weide, 2023). This resource competition directly facilitates violent extremist group recruitment, as organizations like JNIM and DAESH-GS (DAESH in the Greater Sahara) offer protection for herding communities and access to disputed resources in exchange for loyalty and military participation (Victoria & Martinez, 2024; Council on Foreign Relations, 2025). The displacement cascades further compound these dynamics.

For NATO's Military Instrument of Power (MIoP), climate adaptation imposes significant costs. Equipment attrition accelerates in extreme heat and humidity; operational challenges multiply in austere, degraded environments; and defence spending faces pressure as member states redirect resources to domestic climate adaptation and energy transition (Stockholm International Peace Research Institute, 2024; OECD, 2024). The green energy transition, while necessary for strategic autonomy, creates new dependencies and supply chain vulnerabilities. Rare earth minerals, essential for defence electronics, such as lithium, cobalt and nickel become increasingly contested resources (Stockholm International Peace Research Institute, 2024). Terrorist organizations and their state sponsors exploit this competition, targeting mining operations and supply chain infrastructure in fragile states, potentially financing operations through illicit mineral trafficking (World Bank, 2024).

3.4 Emerging Disruptive Technologies: The Accelerating Convergence

The convergence of artificial intelligence, autonomous systems, quantum computing, and biotechnology will “reshape states, societies and armed forces as well

as the character of competition and warfare with unprecedented speed" (NATO Allied Command Transformation, 2023, p. 35). For counter-terrorism, this creates asymmetric vulnerabilities that current doctrine inadequately addresses. NATO's Warfighting Capstone Concept similarly argues that emerging and disruptive technologies (EDTs) will extend the battlespace into new domains and compress decision cycles (NATO Warfighting Capstone Concept, 2021).

AI-enabled terrorist recruitment represents an immediate threat with documented precedent. The DAESH-KP, following the Taliban's return to Afghanistan in 2021 and territorial losses, increasingly relies on AI-based radicalisation tools to differentiate itself from other extremist organisations and maintain ideological cohesion (Global Network on Extremism and Technology, 2025). DAESH-KP distributed an AI-generated news bulletin following the March 2024 Moscow attack on Crocus City Hall, marking a significant paradigm shift in how extremist groups leverage AI (Global Network on Extremism and Technology, 2025; Weimann et al., 2024). Rather than conventional propaganda videos relying on amateur-quality footage, AI-generated bulletins present professionally formatted, multilingual content designed to maximize algorithmic amplification on social media platforms (Weimann et al., 2024). Unlike human recruiters operating during traditional business hours, AI-powered chatbots operate continuously across multiple platforms, engaging in conversations that mimic human interactions while being designed to tailor radicalisation pathways; these systems analyse behavioural triggers and adapt responses based on each individual's ideological inclinations and personal vulnerabilities (Global Network on Extremism and Technology, 2025).

The danger lies in passive recruitment enabled by AI. Traditional recruitment required active engagement by group members; AI-enabled systems can identify vulnerable individuals through their social media activity, engagement patterns, and demonstrated ideological leanings, then automatically initiate targeted recruitment conversations. Data-driven insights from social media behaviour allow extremists to customize propaganda in real-time, making AI-assisted radicalisation significantly more effective than traditional methods (Weimann et al., 2024). DAESH published a comprehensive guide titled "How to Securely Use Generative AI" in 2023, demonstrating strategic adoption of these technologies across their operational spectrum (Global Network on Extremism and Technology, 2025).

Autonomous systems present parallel challenges. The Russo-Ukrainian War has served as an "innovation hub" for drone warfare, accelerating advancements in the scale, speed, and range of drone operations that terrorist groups closely monitor and seek to replicate. First-Person View (FPV) drones have normalized coordinated drone swarms and phased attacks capable of overwhelming existing defences (Rassler & Veilleux-Lepage, 2025). During DAESH's occupation of Mosul, the organization used drones operationally integrated with command-and-control

structures, allowing commanders to monitor attacks in real-time, guide Vehicle-Borne Improvised Explosive Devices (VBIEDs), and direct mortar and artillery fire with unprecedented precision. Drones mapped urban landscapes, enabling suicide attack coordination with accuracy previously impossible. When paired with emerging AI-assisted targeting systems, these capabilities could significantly increase the precision and impact of future terrorist attacks (Rassler, D., & Veilleux-Lepage, Y., 2025).

The diffusion of technology empowers non-state actors to challenge traditional state power in ways NATO doctrine originally conceived for state competitors (NATO Allied Command Transformation, 2023). Terrorist groups already exploit ChatGPT-style tools for recruitment, deepfake generation for disinformation campaigns, and autonomous vehicles for targeted attacks (Weimann et al., 2024; Liang, 2023). Commercial sectors lead innovation in these domains, creating dependence on private actors who may not share NATO's security priorities and operate across jurisdictions with varying regulatory regimes. The low entry costs for acquiring these capabilities be it a smartphone and internet connection suffice for recruitment; commercially available drones can be modified with minimal cost for weapons delivery, fundamentally alter the calculus of terrorist capability development (Liang, 2023).

3.5 Human Networks Empowered: The Shift in Power Locus

Technology-enabled human networks are fundamentally redistributing power away from states and towards non-state actors, reshaping the security environment in ways that legacy institutional frameworks were not designed to address. Social media platforms, encrypted messaging applications, and crowdfunding mechanisms allow terrorist organisations to mobilise resources, coordinate operations, and radicalise individuals across borders with minimal physical footprint or state sponsorship. Cities emerge as “critical nodes for future military operations” where dense populations, critical infrastructure, and information flows converge (NATO Allied Command Transformation, 2023, p. 49). This urban concentration creates dual vulnerabilities: terrorists can inflict mass casualties and economic disruption with relatively limited capabilities, while the information environment becomes congested with competing narratives that complicate state communication and counter-narrative efforts (UNODC, 2024).

Urban density itself creates operational vulnerabilities that terrorist actors systematically exploit. UN research on urban terrorism protection documents how

terrorists have leveraged traffic congestion in Kabul to delay law enforcement response; in densely built environments with limited evacuation routes, a single attack can trigger cascade effects throughout interconnected infrastructure networks that constitute cities' “lifeblood”. The concentration of population in spaces designed for commerce, culture, and transportation creates terrorist targeting opportunities: suicide attacks in crowded shopping districts, vehicle-borne IEDs in congested transport hubs, and mass-casualty attacks in places of worship achieve high-impact effects with minimal planning complexity (UNODC, 2024).

Cognitive warfare, which is targeting perceptions, beliefs, and decision-making processes, becomes as critical as kinetic operations in urban environments. NATO's information instrument faces challenges from “high density of disinformation, signal interference, and diverging values” that complicate attribution and response (NATO Allied Command Transformation, 2024). As NATO's Cognitive Warfare Concept documentation notes, adversaries attempt to undermine public trust through spreading disinformation and confrontational rhetoric online, forming part of broader cognitive warfare strategy (NATO Allied Command Transformation, 2024; Parrish, Armon & Shwartz-Asher, 2024). This threat extends to NATO's operational effectiveness: if terrorist groups successfully manipulate public perception through AI-generated deepfakes showing NATO forces committing war crimes or humanitarian disasters, public will to sustain counter-terrorism operations may erode regardless of actual military necessity or legal justification (Rainero & Tagarev, 2024).

3.6 Scramble for the Commons: Governance Vacuums and Terrorist Exploitation

The global commons—cyberspace, outer space, atmosphere, high seas, and polar regions—are becoming increasingly congested and contested, creating what SFA23 terms “pervasive competition” in insufficiently regulated domains (NATO Allied Command Transformation, 2023, pp. 57–66). Insufficient regulation creates opportunities for terrorist actors to operate with plausible deniability, particularly in cyberspace where attribution remains challenging and legal frameworks remain contested (Sartori & Stefanini, 2022).

Space presents an emerging frontier for terrorist exploitation that current counter-terrorism deliberations in Allied Joint Publication 0.1 barely address. Space-based assets essential for intelligence, surveillance, and reconnaissance (ISR) become targets for adversaries seeking to degrade Allied capability (van Genderen & Pinguet, 2022). More critically, the commercialization of space capabilities means that terrorist groups can purchase satellite services for reconnaissance without direct state sponsorship (van Genderen, Genderen-Moore & Renshaw, 2025). Companies providing commercial satellite communications globally create dual-use vulnerabilities: the same capabilities enabling terrorist communication security also provide them with

resilient, globally accessible networks that evade traditional signals intelligence collection.

Undersea infrastructure faces sabotage threats that could enable terrorist coordination while simultaneously disabling counter-terrorism response capabilities. These cables are carrying over 99 per cent of intercontinental data traffic and critical energy pipelines. A coordinated attack on multiple subsea cables could fragment the internet regionally, isolating targeted communities from external communication while concentrating information flows through limited channels that terrorist networks could exploit. The lack of governance frameworks for emerging domains allows terrorists to exploit legal ambiguities and enforcement gaps at unprecedented scale (World Bank, 2024).

Cyberspace itself remains the archetypal ungoverned commons for terrorist operations. Attribution challenges mean that cyber-terrorism can be conducted with minimal risk of attribution or retaliation (Lehr, 2024). The convergence of terrorist groups with state-sponsored cyber capabilities creates hybrid threats where distinguishing terrorist activity from state action becomes analytically impossible (Sokolowski & Vershinin, 2023; Sartori & Stefanini, 2022). DAESH''s established cyber capabilities and stated intentions to conduct cyberattacks on critical infrastructure represent a merger of terrorist targeting with state-level technical sophistication that NATO's counter-terrorism frameworks were designed to address separately (Sandler, 2015).

3.7 International Order in Transition: Fragmentation and Extremist Opportunity

The rules-based international order (RBIO) is fragmenting, with strategic competitors promoting alternative norms and regimes (North Atlantic Treaty Organization, 2022). This erosion complicates counter-terrorism cooperation, as consensus on definitions, legal frameworks, and response protocols weakens (Pomarede, 2024). Terrorist organisations exploit this fragmentation by operating across jurisdictions with inconsistent legal standards and by aligning with state actors who undermine global counter-terrorism efforts (Shentov & Petrov, 2024).

The rise of geoeconomic blocs and economic decoupling further fragments responses. Sanctions and financial controls become less effective when alternative economic systems emerge (Rainero & Tagarev, 2024). Terrorist financing adapts through decentralized financial systems, cryptocurrencies, and informal economies that circumvent traditional monitoring. Analysis of 2024 illicit cryptocurrency activity reveals that while traditional financing mechanisms (cash, hawalas, money service businesses) remain dominant, terrorist group use of cryptocurrency expanded significantly. DAESH-KP's cryptocurrency role, highlighted in connection with the

March 2024 Moscow attack, signals a growing trend (Smith & Garrett, 2025). The estimated illicit crypto volume for 2024 ranges from roughly USD 44.7 billion to USD 75 billion; while only a small share of overall crypto volume, this represents preferred channels for groups lacking state sponsorship (Chainalysis, 2024). Terrorists prefer blockchains with low transaction fees, smart contracts, and popular stablecoins, particularly the Tron blockchain (around 58 per cent of illicit on-chain activity), Ethereum, and privacy coins like Monero that are difficult to trace (Smith & Garrett, 2025). Cryptocurrency's growing role in terrorism financing, though numerically small, demonstrates terrorist adaptation to emerging economic technologies and suggests acceleration as these systems mature and integrate with mainstream financial infrastructure (Ang, 2025).

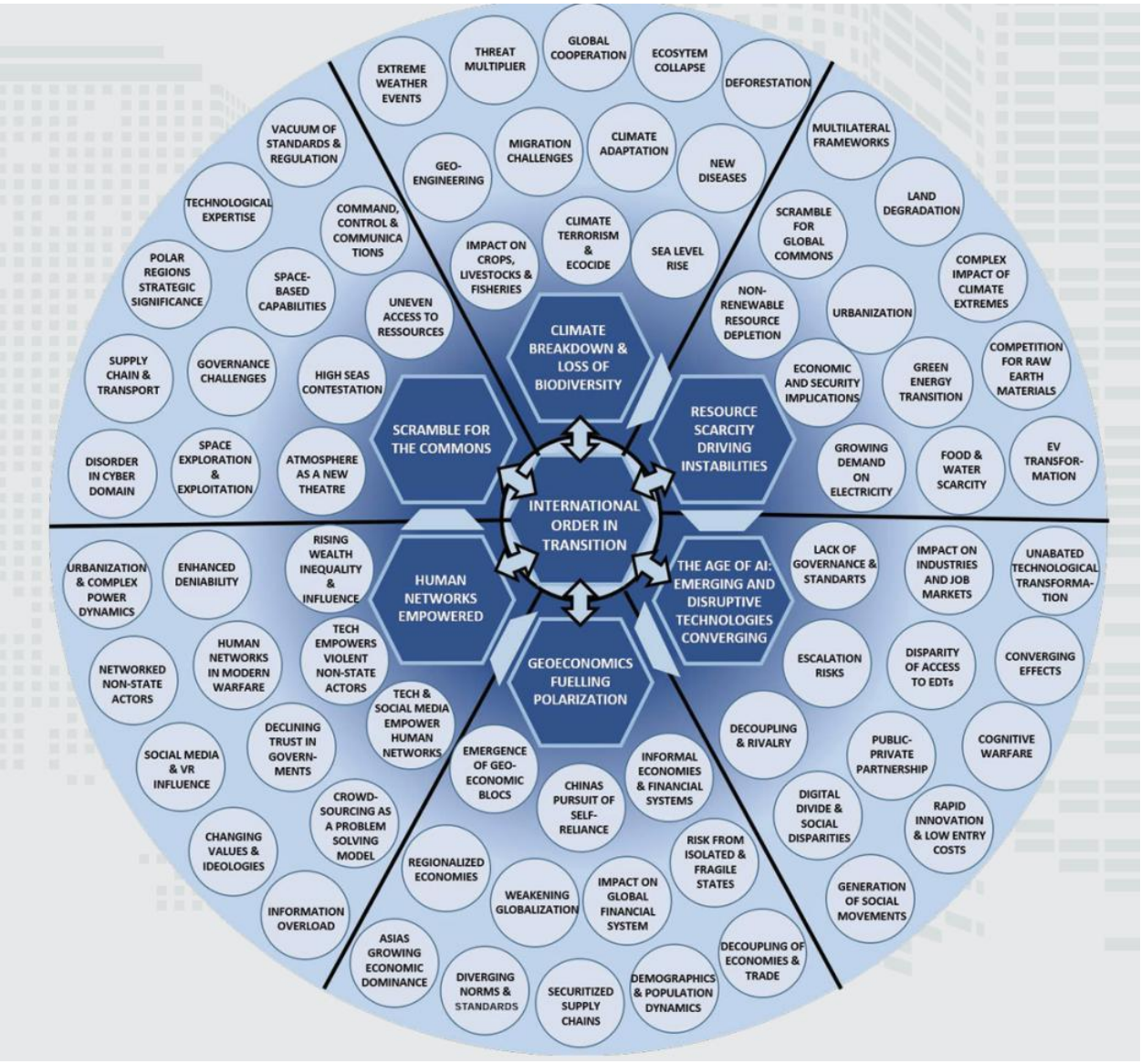


Figure 4: Radar of trends and drivers in the Strategic Foresight Analysis 2023 (Source: NATO Allied Command Transformation 2023)

Taken together, SFA23's seven structural drivers do not operate in isolation but form a compounding, cascading threat environment whose constituent elements reinforce one another in complex feedback loops. Climate breakdown generates the grievances and ungoverned spaces that technology-enabled human networks exploit for recruitment; emerging disruptive technologies amplify the reach and lethality of actors who exploit fractures in the international order; and the scramble for the commons provides the operational cover; in cyberspace, in orbit, and on the ocean floor, within which these actors can increasingly efficiently manoeuvre below the threshold of conventional response. The aggregate effect is a qualitative transformation in the character of terrorism: it may evolve from a predominantly physical, episodic, and geographically bounded phenomenon toward a persistent, multi-domain, and cognitively oriented one that current NATO counter-terrorism frameworks were not designed to address at this scale or speed. Against this backdrop, the following section stress-tests NATO's existing doctrinal and institutional baselines against three distinct future pathways, assessing where current frameworks remain sufficient and where reconceptualisation could be reconsidered.

4. Three Distinct Pathways: Future Scenarios for Counter-Terrorism to 2043

This chapter translates the systemic disruptions identified in SFA23 into three distinct future pathways for counter-terrorism: Pervasive Competition, Fragmenting World, and Adaptive Cooperation. SFA23 established the three distinct pathways as futures trajectories for the evolution of the global security environment into 2043. The pathways are differentiated by two key variables: the degree of structural disruption and the level of international cooperation. The Fragmenting World pathway represents NATO's current baseline security environment as established in the 2022 Strategic Concept, with low disruption and limited cooperation, characterized by existing erosion of the rules-based international order but without major systemic shocks. The Pervasive Competition pathway—assessed as most probable—depicts high disruption and low cooperation, where climate breakdown, resource scarcity, and technology diffusion accelerate structural disruptions while strategic competitors actively undermine global cooperation, forcing NATO to respond in a security environment that is complex, congested, commercialized, contested, and confused. Finally, the Global Cooperation pathway represents the optimistic scenario (low probability but strategically important) in which shifting attitudes of major competitors enable enhanced global coordination on climate mitigation, technology governance, and international stability, though current indicators make this unlikely in the near term.

The utility of such concepts lies in stress-testing NATO’s current doctrinal and institutional baselines (established in Chapter 2) against divergent futures, revealing where existing frameworks like AJP-01 and the 2024 Policy Guidelines are sufficiently robust and where they risk obsolescence, especially in terms of the future of counter-terrorism.

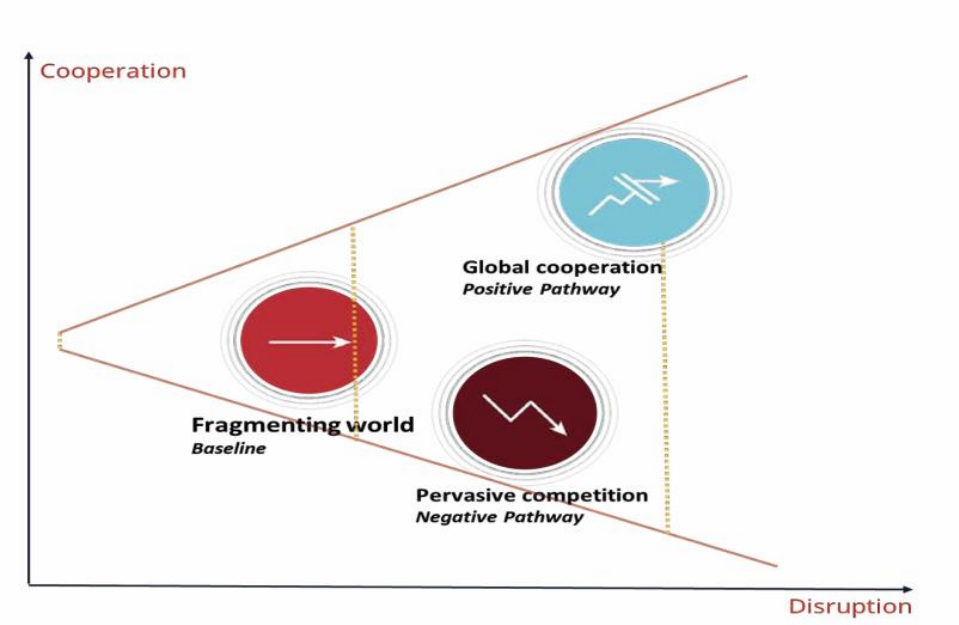


Figure 5: Pathways of the evolving security environment (Source: NATO Allied Command Transformation, 2023)

4.1 Scenario 1: Pervasive Competition (High Disruption, Low Cooperation)

Probability: Most likely. SFA23 identifies this as the core scenario reflecting baseline assumptions.

In this pathway, structural disruptions from climate change, technology, and resource scarcity intensify while strategic competitors actively undermine cooperation on global challenges. The security environment becomes increasingly “complex, congested, commercialized, contested, and confused”. Terrorist actors can operate across a blurred continuum of competition, employing hybrid tactics that combine conventional terrorism with cyberattacks, cognitive warfare, and exploitation of governance gaps. States weakened by climate impacts and economic competition lose capacity to govern effectively, creating ungoverned spaces where terrorist networks establish operational bases. Rather than fighting against a centralized enemy, NATO confronts a diffuse ecosystem of threats simultaneously operating at tactical (kinetic attacks), operational (logistics and recruitment networks), and strategic (narrative and political) levels (also mentioned in Pomarede, 2024).

In this scenario, terrorism becomes increasingly embedded within broader hybrid warfare strategies. Unlike past terrorism that sought to provoke emotional reaction and policy change through spectacular violence, pervasive-competition terrorism functions as a tool within broader competitive strategies. Adversaries of the Alliance may sponsor terrorist proxies not primarily to maximize casualties but to generate instability that constrains NATO's freedom of action, creates recruitment

pools for their own information warfare operations, and justifies internal security crackdowns that consolidate state control. Terrorist groups themselves become more sophisticated, operating as networked enterprises rather than hierarchical organisations, with distributed decision-making that mimics commercial technology platforms more than military command structures.

Critical Challenges for Counter-Terrorism Doctrine and Practice

Attribution and Multi-Source Threat Confusion: The density of state and non-state actors simultaneously engaging in hostile activities creates attribution challenges that exceed current legal and technical frameworks (also pointed out in Lehr, 2024). When a drone attack on NATO infrastructure could originate from a terrorist group, a criminal organisation, a regional proxy force, or a great power using terrorist-style tactics for plausible deniability, response options diverge dramatically (Rassler & Veilleux-Lepage, 2025). Current AJP-01 guidance on the conflict triangle (contradiction–attitude–behaviour) assumes a discernible adversary against which counter-messaging and deterrence can be directed. In pervasive competition, the “adversary” becomes ambiguous. Terrorist groups using AI-generated deepfakes to impersonate state actors, autonomous systems that obscure human agency, and encrypted networks that prevent origin identification place attribution burden on NATO's intelligence apparatus at precisely the moment competing information operations aim to undermine public trust in intelligence institutions.

Capability Gap and Commercial Dependence: NATO's military instrument faces significant constraints from climate adaptation costs diverting defence resources, ageing societies reducing military participation, and skilled workforce shortages competing with lucrative commercial technology sectors (reinforced by other studies, like Stockholm International Peace Research Institute, 2024; OECD, 2024). The commercial sector leads innovation in AI, robotics, and autonomous systems, creating structural dependence on private actors who operate beyond NATO's control and often across competing regulatory regimes. When technologically empowered super wealthy individuals can unilaterally restrict access to Starlink satellite communications, as occurred during the Ukraine war, this demonstrates how commercial technology concentration creates vulnerabilities in NATO's operational freedom (RUSI, 2024). A terrorist group or state sponsor could acquire similar leverage through commercial platforms, constraining Alliance operational options. Moreover, private AI systems trained on global datasets encode values and biases not aligned with NATO's strategic objectives. A generative AI system trained to optimize engagement metrics will amplify the most sensational terrorist narratives regardless of NATO counter-messaging, creating an information environment where terrorism's psychological impact expands faster than counter-terrorism's ability to mitigate it (Weimann et al., 2024).

Cognitive Dimension Under-Addressed: Current counter-terrorism guidelines inadequately address cognitive warfare's scale and personalization. AI-enabled information campaigns target individuals with “highly personalized and contextualized digital and media information campaigns at mass scale,” eroding societal resilience and political will to sustain counter-terrorism operations (NATO Allied Command Transformation, 2023, p. 49; Parrish et al., 2024). NATO's strategic communications framework, designed for broadcasting coherent messages to mass audiences, may prove inadequate for countering individually-targeted disinformation. When social media algorithms learn that an individual holds moderate xenophobic or conspiratorial views, they can progressively expose that person to increasingly radical content, eventually radicalising them through automated processes requiring no human recruiter (Shirtcliff et al., 2024). Terrorism, previously studied as recruitment through social networks and charismatic leadership, becomes a phenomenon that can emerge through algorithmic manipulation and personalized content delivery.

Governance Deficit in Emerging Domains: The scramble for commons outpaces regulatory frameworks. Terrorist exploitation of space-based assets, undersea infrastructure, and atmospheric domains occurs in legal vacuums where national sovereignty claims conflict with international law principles and technical capacity to enforce restrictions remains limited. When space cybersecurity governance remains fragmented across multiple government agencies, the challenge of securing space-based counter-terrorism ISR assets becomes intractable. A terrorist group could purchase commercial satellite services, receive intelligence from sympathetic state actors, and launch coordinated attacks on NATO facilities with warning time compressed below response capability.

Opportunities and Adaptive Responses

Technology Integration and Innovation: NATO can leverage AI and autonomous systems for threat detection and operational acceleration, albeit requiring new public-private partnerships and governance models that transcend traditional military-industry relationships. If NATO establishes formal partnerships with leading AI companies on counter-terrorism algorithms, with explicit security classification and oversight arrangements, the Alliance could develop detection systems that match or exceed terrorist groups' sophisticated recruiting and targeting capabilities. COE-DAT could establish innovation labs partnering with technology companies to anticipate terrorist technology adoption and develop countermeasures, thus moving from reactive vulnerability patching to proactive capability development. However, this requires accepting that NATO cannot maintain unilateral technological superiority; instead, NATO must develop adaptive systems that continuously update as terrorist groups innovate.

Resilience Focus and Multi-Level Integration: The emphasis on national resilience in the 2024 Guidelines aligns with climate adaptation needs, creating synergies between counter-terrorism and societal resilience. Rather than viewing counter-terrorism as separate from climate adaptation, NATO can pursue these agendas in an integrated manner. Resilience-building in fragile regions vulnerable to climate-driven extremism recruitment becomes a counter-terrorism priority. Capacity-building for water resource management and agricultural adaptation in the Sahel simultaneously reduces extremist recruitment pools by providing alternative livelihoods. This approach could convert a potential trade-off, ie., climate adaptation requiring resources versus counter-terrorism requiring resources, into complementary missions that reinforce each other.

Multi-Domain Operations Framework: NATO's evolving doctrine for multi-domain operations provides a framework for integrating counter-terrorism across physical, virtual, and cognitive dimensions. Rather than conducting kinetic operations (special forces raids on terrorist bases), cyber operations (network disruption), and information operations (counter-narratives) as separate campaigns, multi-domain integration orchestrates these simultaneously to achieve synergistic effects. A kinetic operation against a terrorist leader could be synchronized with cyber operations disrupting their financial networks and cognitive operations delegitimizing their authority among their following, compressing the terrorist organization's ability to respond or reconstitute. This integration requires doctrinal evolution that AJP-01 initiates but counter-terrorism guidance has not yet fully operationalized.

4.2 Scenario 2: Fragmenting World (Baseline Continuation Without Systemic Transformation)

Probability Assessment: Moderate. This scenario represents continuation of current trajectory without major systemic shocks (NATO Allied Command Transformation, 2023).

In this scenario, the security environment described in NATO's 2022 Strategic Concept continues evolving without fundamental shocks that would force either greater cooperation or cascading collapse. Russian aggression persists as regional challenge rather than systemic threat; China expands its footprint gradually through economic and technological means; terrorism remains a persistent asymmetric threat requiring sustained attention but not existential concern. Cooperation remains limited to traditional Alliance structures and established partnerships, with ad hoc arrangements addressing specific crises. International order fragments into competing spheres of influence but without triggering multipolar conflict or complete institutional collapse (also in National Intelligence Council, 2021). This is the most strategically comfortable scenario for NATO, as it preserves existing institutional arrangements and operational patterns while requiring incremental rather than fundamental adaptation.

Key Characteristics and Challenges

The fragmented world scenario assumes that current counter-terrorism challenges persist without fundamental transformation. Regional terrorist groups maintain regional focus; foreign terrorist fighters continue flowing to conflict zones in the Middle East and Africa but without achieving massive scale or technological sophistication; cyber-terrorism remains disruptive but below critical infrastructure collapse threshold; recruitment continues through social media but without achieving AI-enabled personalization at scale. Defence budgets remain contested but sufficient for current commitments; NATO enlargement stabilizes; technology diffusion continues but without revolutionary change in terrorist capability.

Institutional inertia becomes a central challenge. NATO's counter-terrorism architecture may fail to adapt sufficiently to incremental technological changes, leaving capability gaps that terrorist actors exploit through “low and slow” innovation adoption. Drone terrorism illustrates this risk. DAESH's drone innovations in 2015–2017 represented rapid capability adoption; in a fragmented world scenario, subsequent terrorist groups adopt these proven tactics gradually over 5–10 years, refining techniques and increasing range and payload incrementally. By the time NATO recognizes the magnitude of the evolved threat—perhaps when coordinated drone swarms conduct mass-casualty attacks—the technological and doctrinal adaptation required exceeds NATO's response capacity.

Resource competition reinforces inertia. Defence budgets face persistent pressure from competing domestic priorities, such as healthcare, pensions, education, as domestic politics emphasize social spending over military capability (OECD, 2024). The “lowest common denominator” effect in NATO's consensus-based decision-making slows response to novel threats; when one member state prioritizes counter-terrorism while another prioritizes peer-state deterrence, consensus doctrine reflects the lower priority rather than the highest threat. Investment in emerging counter-terrorism capabilities (AI-based detection, autonomous counter-drone systems, cognitive resilience programs) competes with traditional capability modernisation, potentially leaving both areas under-resourced.

Limited cooperation constrains capacity-building in fragile states where terrorism takes root, particularly in NATO's southern neighbourhood. The Sahel region's escalating terrorism crisis demonstrates this dynamic. Terrorist-linked violence in the region has killed many thousands annually, as JNIM, DAESH-GS, and ISWAP expand influence in weakly governed areas. NATO's capacity-building efforts in African partner states remain limited compared to resource requirements. Without fundamental expansion of NATO's training footprint or transformation of partner-state governance capacity, fragmented world scenario sees terrorism's geographic spread and intensity increase despite NATO's counter-terrorism efforts.

Opportunities and Institutional Learning

At the same time, fragmented world offers advantages. Doctrinal continuity allows gradual refinement of proven concepts like the comprehensive approach, behaviour-centric operations, and mission command. COE-DAT could further deepen training programs, expand Mobile Training Teams, and progressively improve integration between NATO counter-terrorism operations and partner capacity-building. Incremental improvement, while less dramatic than transformation, may prove sufficient if terrorist threats evolve correspondingly slowly.

Predictable threat environment enables targeted capability development in areas of demonstrated NATO advantage. Special operations forces, intelligence fusion centres, and interagency coordination mechanisms can be progressively improved. NATO's long-term presence in the Western Balkans provides a model: sustained engagement has helped prevent renewed large-scale violence and curtailed extremist influences, albeit imperfectly. Similar patient, long-term investment in Sahel partner states could gradually build institutional capacity that prevents terrorist organizations from establishing permanent safe havens.

4.3 Scenario 3: Adaptive Cooperation (Low Disruption, High International Cooperation)

Probability Assessment: Low probability. Strategic competitors maintain adversarial posture.

Strategic Narrative: This optimistic scenario assumes global coordination emerges to address climate change, resource scarcity, and technology governance. New arms control frameworks appear for emerging and disruptive technologies, and the Rules Based International Order is revitalized through reformed international institutions. Terrorism is explicitly treated as a shared global challenge rather than a tool of state strategy. International coordination on counter-terrorism financing creates unified regulatory frameworks closing cryptocurrency and informal economy loopholes. Technology governance frameworks prevent civilian access to hazardous technologies, restricting terrorist exploitation while enabling NATO's legitimate use. This scenario assumes that the international system learns from climate impacts, pandemics, and current conflicts, implementing institutional reforms that enable coordinated responses to global challenges.

Challenges for Counter-Terrorism

Over-institutionalisation may generate bureaucratic processes that slow rapid response to terrorist threats, particularly those requiring immediate operational action. When terrorism response requires coordination across the UN Security Council,

international legal frameworks, and consensus-based NATO decision-making, response times may exceed terrorist decision cycles.

Division of labour among international organisations might lead NATO to neglect core military counter-terrorism capabilities, assuming civilian agencies will lead. If the UN Office of Counter-Terrorism takes lead on prevention and rehabilitation, the EU on radicalization and law enforcement, and NATO on only the most kinetic operations, NATO's specialized counter-terrorism skill sets could atrophy over time.

Strengthened international law and human rights frameworks could limit intelligence collection and operational flexibility in counter-terrorism missions. Enhanced privacy protections in data collection, restrictions on bulk surveillance, and increased litigation risks from human-rights courts might constrain intelligence services' ability to identify and track terrorist networks. Counter-terrorism operations in densely populated civilian areas face stricter constraints under international humanitarian law. While these normative developments reflect important values, they also create operational asymmetries that terrorist groups unconstrained by similar rules exploit.

Opportunities in Cooperative Environment

Coordinated diplomatic, economic, military, and intelligence instruments could systematically dismantle terrorist networks globally. Intelligence shared freely across allied services eliminates terrorist logistics networks' ability to exploit different regulatory or enforcement regimes. Economic instruments prevent terrorist financing through comprehensive sanctions and controlled technology access. Military intervention against remaining terrorist bases operates under international sanction and coordination. Rather than NATO fighting terrorism piecemeal across multiple regional conflicts, a globally coordinated campaign systematically eliminates terrorist organizations' capacity to operate.

Global standards for AI, autonomous systems, and biotechnology could restrict terrorist access while enabling NATO's legitimate use. International oversight mechanisms verifying compliance prevent terrorist acquisition of prohibited technologies, while NATO retains access to frontier technologies for defensive purposes. This reverses the current trajectory where technology diffusion empowers non-state actors; instead, governance frameworks create renewed state advantage.

International climate adaptation funding and governance support could substantially reduce fragility and terrorism recruitment pools. When climate adaptation enables Sahel communities to maintain agricultural productivity despite changing precipitation patterns, when resource scarcity is managed through international frameworks rather than violent competition, and when displaced populations receive

assistance rather than becoming recruitment targets, terrorism's structural drivers diminish.

5. Conclusions and recommendations

NATO's counter-terrorism frameworks such as AJP-01's doctrinal tenets, the 2024 Policy Guidelines' three pillars of awareness, capabilities, and engagement, and COE-DAT's contribution through training and research provide necessary but insufficient foundation for addressing counter-terrorism challenges through 2043. The pervasive competition scenario, assessed as most probable by SFA23, will require fundamental reconceptualization of counter-terrorism related considerations and a strategy around several critical emerging themes.

The Alliance must evolve cognitive warfare from emerging concept to core doctrinal domain with equivalent priority to kinetic operations. This requires developing detection and mitigation capabilities for AI-enabled influence operations, building societal resilience frameworks, and integrating cognitive considerations into all counter-terrorism operation planning. COE-DAT's and NATO ACT's Cognitive Warfare Concept development represent important steps that require acceleration and institutionalization.

NATO should also expand counter-terrorism frameworks beyond state-centric approaches to address distributed networks and ungoverned spaces where terrorism increasingly takes root. This may require novel partnerships with civil society, technology companies, and community organizations that extend beyond traditional military partnerships. The comprehensive approach must genuinely comprehend non-military actors as essential partners.

It is imperative, the climate adaptation must be integrated into counter-terrorism strategy as fundamental driver reduction rather than peripheral resilience concern. NATO should establish explicit linkages between counter-terrorism capacity-building and climate adaptation funding in fragile regions, treating them as complementary rather than competitive priorities. This requires coordination across NATO, EU, World Bank, UN and other relevant multilateral frameworks that transcends traditional security silos.

A counter-terrorism doctrine could also be considered beyond the existing framework of relevant Allied Joint Publications, and CT Policy Guidelines, and integrated with hybrid threats response planning at all levels, recognizing that terrorist activity often serves broader competitive strategies. Operations should be designed with recognition that tactical terrorism may achieve strategic effects through integration with information, economic, and diplomatic components of hybrid threats.

NATO should consider to further develop technology governance frameworks that address dual-use innovation diffusion, working with commercial technology companies, international regulatory bodies, and law enforcement to prevent terrorist exploitation while preserving beneficial innovation. This represents evolution of counter-terrorism from operational security problem to governance and innovation policy domain – one in which both the research capacity of relevant COEs and the concept development capacity of NATO ACT can play a pivotal, leading role.

COE-DAT should play increasingly important role in this transformation, but its impact will depend on whether its insights translate into NATO doctrine and defence planning. The Centre's recent accreditation and expanded research agenda provide opportunity for this translation, yet structural tensions between COE independence and NATO's hierarchical command structures remain. Success requires explicit mechanisms for integrating COE-DAT research into NATO's planning processes, ensuring that institutional innovation at the Centre translates to operational innovation across the Alliance.

The future of counter-terrorism will be determined by the Alliance's capacity to adapt faster than terrorist networks themselves evolve, to address the structural drivers generating terrorism, and to maintain societal resilience against both terrorist violence and the cognitive warfare that amplifies its effects. NATO's doctrinal frameworks provide starting points for this adaptation. The challenge ahead is translating futures insights into doctrines, strategy, then capability, and subsequently into effective operations that preserve Alliance security while respecting the principles and values upon which NATO was founded.

References

Ang, A. (2025). Cryptocurrency's growing role in terrorist financing. TRM Labs Asia-Pacific Analysis.

Chainalysis. (2024). Assessing terrorism financing on-chain: Why it is crucial and complex. Blockchain Analysis Report.

Combaz, E. (2021). Climate change, health, and conflict in Africa's arc of instability. Conflict Trends, 5, 31-40.

Council on Foreign Relations. (2025). Violent extremism in the Sahel: Global conflict tracker. Retrieved from https://www.cfr.org/global-conflict-tracker

Dittmer, P., & Wachs, S. (2024). From climate conflicts to environmental peacebuilding: Exploring local dimensions. Environmental Research Letters, 19(2).

European Commission. (2024). Report on the emerging patterns of misuse of technology by terrorist actors. Council of Europe Report.

Felbab-Brown, V. & Renwick, D. (2025). Violent extremism in the Sahel. Council on Foreign Relations Global Conflict Tracker.

Genderen, P. van & Pinguet, L. (2022). Space cybersecurity governance: Assessing policies and frameworks. Oxford Cybersecurity, 1(1).

Hillebrand, C. (2022). Strategic foresight in NATO and strategic commands: An analysis of methodologies and institutional architecture. Defence Science Review, 8(4).

International Panel on the Impacts of Climate Change. (2025). Climate change, conflict and displacement in the Sahel. Environmental Security Journal.

Jarvis, Lee (2024). Three waves of critical terrorism studies: agenda setting, elaboration, problematization. Critical Studies on Terrorism, 17:3, 463-487,

Kouvo, S., Kurki, L., & Solanki, G. (2025). Climate change, terrorism, and preventing violent extremism: The security-development nexus in Mauritania. Preventing Violent Extremism Programme - Germany-UNICRI Partnership.

Kuntzman, K. & Scheiber, N. (2024). Transparent communication in counter-terrorism policy: Does transparency increase public support and trust in terrorism prevention programmes? Terrorism and Political Violence, 36(3).

Kurz, H. (2024). EU space security: An 8-step online discourse analysis to decode hybrid threats. Space Policy, 68, 101487.

Lehr, P. (2024). The future of counter-terrorism in Europe: The need to be lost in the correct direction. European Security Review, 22(4).

Lipin, I. (2024). The Arctic front of the global hybrid warfare. Hybrid Threats Research, 9(2).

NATO Allied Command Transformation. (2023). Strategic Foresight Analysis 2023. NATO ACT Publications.

NATO Allied Command Transformation. (2024). Cognitive warfare concept to combat disinformation. NATO ACT Press Release.

NATO Allied Command Transformation (2021). NATO Warfighting Capstone Concept

NATO Defence Against Terrorism Centre of Excellence. (2024). The role of counter-terrorism in hybrid warfare. COE-DAT Research Publications.

NATO Defence Against Terrorism Centre of Excellence. (2024). 2025 Centre of Excellence catalogue. NATO ACT Publications.

NATO Chief Scientist Research Report on Cognitive Warfare (2025). NATO Science & Technology Organization.

NATO Office of Public Diplomacy. (2024). NATO's policy guidelines on counter-terrorism. NATO Official Texts and Resources, Washington Summit Declaration.

NATO Office of Public Diplomacy. (2024). Countering terrorism. NATO Topic Retrieved from https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism

NATO Office of Public Diplomacy. (2024). Countering hybrid threats. NATO Topic. Retrieved from https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

NATO Office of Public Diplomacy. (2024). NATO centres of excellence – Defence against terrorism (COE-DAT). NATO Centres of Excellence Topic.

NATO Standardization Office. (2022). Allied joint publication AJP-01: Allied joint doctrine. Edition F, Version 1.

NATO Warfighting Capstone Concept. (2021). NATO Strategic Concepts.

National Intelligence Council. (2021). Global trends 2040. U.S. Office of Director of National Intelligence.

OECD. (2024). Climate security nexus: Policy responses in fragile and conflict-affected states. Climate Change and Security Working Paper.

Parrish, J., Armon, K., & Shwartz-Asher, D. (2024). Cognitive warfare to dominate and redefine adversary realities: Implications for U.S. special operations forces. Journal of Special Operations, 37(2).

Pomarede, E. (2024). Deadly ambiguities: NATO and the politics of counter-terrorism in international organizations after 9/11. Security Dialogue, 55(6), 588–606.

Przeworski, A. (2020). NATO resilience decision support model: Dynamic modeling for resilience measurement. Applied Sciences, 10(8), 2639.

Quillian, L. & Campbell, M. (2025). Climate change, violent extremism, and the role of the international community. Global Security Review, 12(1).

Rainero, L. & Tagarev, T. (2024). Countering hybrid threats: Challenges and the role of defence science. Defence Science Review, 9(3).

Rassler, D., & Veilleux-Lepage, Y. (2025). On the horizon: The Ukraine war and the evolving threat of drone terrorism. CTC Sentinel, 18(3).

Renwick, D. (2024). Violent extremism in the Sahel. Council on Foreign Relations, Global Conflict Tracker Analysis.

Rodiles, A. (2022). Making sense of violent extremism. AJIL Unbound, 116, 230–235.

RUSI. (2024). The future operating environment: Warfare development and strategic foresight. Royal United Services Institute Publication.

Sandler, T. (2015). Terrorism and counterterrorism: An overview. Oxford Economic Papers, 67(1), 1-20.

Sakamoto, S. & Gearan, M. (2024). Early identification of threats as means of fighting against hybrid warfare. Journal of Strategic Security Studies, 8(2).

Sartori, A. & Stefanini, R. (2022). Countermeasures for hybrid threats: The experience of the European Union and its member states. Journal of European Security, 31(3).

Shentov, O. & Petrov, A. (2024). NATO's strategies for responding to hybrid conflicts. Barcelona Centre for International Affairs.

Schori Liang, C. (2023). Terrorist digitals: Preventing terrorists from using emerging technologies. In Institute for Economics and Peace, Global Terrorism Index 2023

Smith, M. & Garrett, B. (2025). Illicit crypto volume and terrorist financing in 2024: TRM Labs analysis. Strait Times Business Report.

Sokolowski, P. & Vershinin, V. (2023). Three perspectives on hybrid warfare: NATO, Russia, and the European Union. Journal of Strategic Studies, 46(1), 45-72.

Stockholm International Peace Research Institute. (2024). Resource scarcity and the shifting dynamics of global security. SIPRI Strategic Analysis Report.

Stokes, J. & Noy, S. (2023). Climate change and terrorism: The nexus in West Africa. Journal of Environmental Security, 11(3).

Sydes, M., Hine, L., Higginson, A., McEwan, J., Dugan, L., & Mazerolle, L. (2023). Criminal justice interventions for preventing radicalisation, violent extremism and terrorism: An evidence and gap map. Campbell Systematic Reviews, 19, e1366.

UN Office of Counter-Terrorism. (2024). Protecting urban centres from terrorist attacks. Retrieved from https://www.un.org/counterterrorism/

UNODC. (2024). Protecting urban centres from terrorist attacks: Good practices guide, Module 2. UN Office on Drugs and Crime Publications.

van Genderen, P., Genderen-Moore, K., & Renshaw, S. (2025). Space cybersecurity governance: Assessing policies and frameworks in view of the future European space legislation. Oxford Cybersecurity, 11(1).

Victoria, A. & Martinez, L. (2024). Violence, poverty and the global security dilemma in the Sahel region. Health & Social Review Publishing, 18(4).

Vision of Humanity Institute. (2025). Climate change and terrorism: Potential implications for prevention and counter-violent extremism. Global Peace Index Special Report.

Visser, S. & Weide, R. (2023). Vicious circles: Violence, vulnerability, and climate change. Annual Review of Environment and Resources, 48, 215-242.

Weimann, G., Pack, A. T., Sulciner, R., Scheinin, J., Rapaport, G., & Diaz, D. (2024). Generating terror: The risks of generative AI exploitation. *CTC Sentinel*, *17*(1).

World Bank. (2024). Assessing climate change risks in fragile and conflict-affected states. Climate Risk Report.

Conclusion

The Next Battlespace: Multi-Domain Terrorism in a Hyperconnected World

Dr. Christina Schori Liang

This volume has demonstrated that the modern terrorist landscape is fluid, adaptive, and increasingly shaped by its geopolitical and digital environment. Terrorism continues to evolve just as it did in the aftermath of the 9/11 attack which fundamentally altered the global security landscape, unleashing the campaign designated as the “War on Terror.” These terrorist attacks galvanized an unprecedented international response, with governments worldwide mobilizing military forces, intelligence agencies, law enforcement organizations, and diplomatic institutions in a coordinated effort to dismantle terrorist networks. A `Coalition of the Willing` designed to be a broad international counterterrorism partnership that involved dozens of nations helped expand intelligence sharing, strengthen legal frameworks, enhance border security while simultaneously conducting multinational operations. This response was unprecedent with so many countries collaborating so extensively against a common non-state adversary. However, it is difficult to claim that this wide-ranging response was effective. The US and its allies were only able to contain terrorism but not entirely defeat it. Terrorism has not been vanquished, instead, it adapted, proliferated, and expanded into new regions and domains, continuing to disrupt the lives of millions of people across the Middle East, Africa, Asia, Europe, and Oceania.

The fallout from the Overseas Contingency Operations (OCO) demonstrated a central lesson for policymakers and strategists alike: while terrorist organizations can be degraded or even temporarily destroyed, terrorists and the ideology of terrorism itself has proven remarkably resilient, continuously evolving in response to political, technological, and societal change. New affiliates emerged across Africa, the Middle East, and Asia underscoring that terrorism is not a problem that can be permanently eliminated through military means alone but instead demands a multipronged domestic and international response ranging from development assistance to prevention to resilience. At the same time, counterterrorism efforts will need persistent attention on how specific groups are evolving. This needs to be done in order to recalibrate and realign the most appropriate responses. At the same time experts must also focus their attention on how the threat will continue to evolve with strategic anticipation.

The first chapter of the volume by Dr. Christina Schori Liang outlines the “Key Global Trends Shaping NATO’s Strategic Challenge to Counter Terrorism.” She maintains that technology will shape our future in more ways than we can imagine—not only transforming the world around us but also redefining who we are and what we are capable of becoming. In the coming decades, the NATO alliance will face significant challenges stemming from five major global trends: rising national populism; profound transformations in the technological landscape; innovations in next-generation warfare; the resurgence of great-power competition; and the increasing fragmentation of the rules-based international order. Collectively, these dynamics will reshape the strategic environment in which NATO operates and will place a growing strain on its existing doctrines and institutional capacities.

The world has been galvanized by renewed great-power competition alongside rapid technological innovation, which will fundamentally alter the entire global security apparatus in profound ways. At the same time, the rapid democratization of advanced technologies is revising the terrorist threat by empowering non-state actors with capabilities once reserved for states. Increasingly technologies including AI-enabled technologies have become more accessible and affordable, allowing terrorists to broaden their ability to communicate, recruit, finance, and disseminate propaganda while at the same time expanding their ability to conduct AI-, cyber- and kinetically-enabled physical and digital attacks. The diffusion of artificial intelligence tools, and the expansion of encrypted communications, cryptocurrencies, and commercial drones are just a few examples of how technological innovation is reinforcing the asymmetric nature of terrorism. Simultaneously countries have become increasingly dependent on a globally connected infrastructure from subsea data cables to nuclear power stations to satellites which has collectively expanded the attack vectors for malevolent terrorist actors to attack.

In the second chapter, Professor John Arquilla describes “What’s Next for Terrorist Strategies.,” He argues that our understanding of terrorism, and of the courses of action terrorist organizations may pursue, is enhanced when terrorism is understood as a form of warfare. This perspective provides a useful framework for considering how terrorist strategies may evolve. Like states engaged in conflict, terrorist organizations make strategic choices concerning both the scope and scale of their operations.

Osama bin Laden’s conception of striking the “far enemy” illustrates one end of this spectrum. The attacks of September 11, 2001, represented an effort to conduct operations on an exceptionally large scale, resulting in the loss of thousands of lives and economic consequences extending into the hundreds of billions of dollars. More recently, however, many terrorist organizations appear to have adopted a strategy more consistent with the ideas advanced by Abu Mus’ab al-Suri, emphasizing smaller-

scale attacks that can nevertheless be dispersed across a wide geographic area. In this approach, strategic effect derives less from the magnitude of individual attacks than from their replication across multiple locations.

The predominance of this approach does not, however, preclude a future shift in terrorist strategy. While al-Suri's concept of "scaling out" has provided a useful framework for understanding the diffusion of terrorist violence, terrorist organizations may also seek, under certain circumstances, to "scale up" the intensity and consequences of their operations. Developments in Afghanistan, the continuing presence of extremist organizations with highly destructive objectives, and the increasing accessibility of advanced technologies raise questions about whether the potential scale of terrorist violence could increase in the future. Emerging capabilities in fields such as biotechnology, introduce new and more dangerous forms of risk that were considerably less accessible to non-state actors in earlier periods.

These possibilities should not be understood as predictions, but rather as considerations that underscore the importance of examining terrorism through a strategic lens. The scale of terrorism can be assessed not only by the number of lives lost in individual attacks, but also by the geographic reach of operations and their broader economic and societal consequences. Understanding how terrorist organizations conceive of scale—and how technological, political, and organizational developments may alter those calculations—will therefore remain an important component of anticipating the future evolution of terrorism.

In the third chapter on "Unconventional Terrorism: Future Trends in the Nuclear and Maritime Domains," Professor Justin Hastings forecasts possible developments in these two domains. He argues that critical infrastructure in the maritime and nuclear domains will serve as both targets and force multipliers for terrorist attacks, and that those emerging technologies, particularly drones and technologies embedded in maritime and nuclear infrastructure will create some new opportunities for violent non-state threats. The nature of maritime infrastructure – ports, sea lanes, and global shipping networks, along with technological trends in shipping, will make attacking easier, and increase the disruption caused by well-placed terrorist attacks especially in places such as chokepoints and heavily trafficked sea lanes. At the same time the expansion of nuclear infrastructure, the ready availability of radioactive sources, and the increasing importance of commercial facilities will make disruptive attacks more attractive for terrorists, but not necessarily deadlier.

In Chapter four, Dr. Vanda Felbab-Brown and Diana Paz Garcia forecast the "Future of the Terror-Crime Nexus." They argue that emerging technologies are likely to fundamentally reshape—and in many cases weaken—the traditional nexus between organized crime and terrorism. Historically, cooperation between these actors has been driven by shared dependence on territorial control, labor-intensive

operations, logistical networks, and mutual protection. However, advances in artificial intelligence, cyber capabilities, additive manufacturing, autonomous systems, and digital finance are enabling both criminal and terrorist organizations to operate with greater autonomy and reduced reliance on territory, manpower, and transnational supply chains. As illicit revenue generation becomes increasingly digital and operations more automated, data, digital infrastructure, and cybersecurity are poised to replace territory as key strategic assets for many violent non-state actors. Although some terrorist groups will continue to pursue territorial control as a core ideological objective, for many others—and for organized crime—state sponsorship may become more valuable than crime-terror collaboration, as states can provide advanced technologies, intelligence, and safe havens that criminal networks cannot. The authors argue that counterterrorism and counter-crime strategies must adapt accordingly by prioritizing the protection of digital infrastructure, the governance of emerging technologies such as additive manufacturing and AI, and the socioeconomic consequences of technological disruption that could expand recruitment into violent non-state groups.

In the fifth chapter on “Transnational Terrorism in Africa: Mapping A New Role for NATO on the Continent,” Dr. Christina Schori Liang highlights how Africa has become the global epicenter of terrorism, with the Sahel now experiencing the highest levels of terrorist violence worldwide. The expansion of violent extremism reflects the interaction of weak governance, political instability, climate change, demographic pressures, porous borders, and the convergence of terrorism with transnational organized crime. At the same time, technological advances have become force multipliers, enabling terrorist organizations to exploit cybercrime, encrypted communications, drones, digital propaganda, and cryptocurrency to strengthen recruitment, financing, intelligence gathering, and cross-border operations.

The evolution of terrorism in West Africa illustrates a shift from fragmented militant groups to highly adaptive and decentralized insurgent networks embedded within local conflicts while maintaining transnational connections. Although post-9/11 military-led counterterrorism campaigns achieved important tactical successes, they failed to address the structural conditions that sustain violent extremism, including fragile institutions, weak governance, socioeconomic exclusion, and regional instability.

Africa's growing demographic, economic, and geopolitical importance makes the continent central to European and transatlantic security. Addressing these challenges requires moving beyond military operations toward comprehensive approaches that strengthen governance, resilience, and long-term institutional capacity. Consistent with the African Union's principle of "African solutions to African problems," sustainable security depends on African-led initiatives supported by regional organizations such as the African Union, ECOWAS, the East African

Community (EAC), and IGAD. Within this framework, NATO's comparative advantage lies in supporting African partners through intelligence sharing, capacity building, maritime security, technological cooperation, and institutional development while fully respecting African ownership and sovereignty. Such partnerships can strengthen resilience against terrorism, organised crime, cyber threats, and the misuse of emerging technologies, contributing to long-term stability, regional prosperity, and collective security.

In the sixth chapter Professor Giray Sadık describes '*Terrorists with Drones: Exploring the Effects of Lethal Autonomy on the Future of Counterterrorism.*' The rapid proliferation of unmanned aerial systems (UAS), autonomous technologies, and artificial intelligence is transforming the future terrorist threat landscape by lowering barriers to entry while increasing the potential scale, precision, and lethality of attacks. Terrorist organizations are increasingly capable of exploiting commercially available drones, autonomous systems, and emerging technologies to conduct asymmetric operations against stronger adversaries. Three major challenges are emerging: the growing advantage of attackers due to the affordability and adaptability of drone technologies, the difficulty of developing effective countermeasures against rapidly evolving systems, and the need for international governance frameworks to address the risks posed by lethal autonomous weapons systems (LAWS).

The vulnerability of critical infrastructure represents a significant concern for NATO Allies and partners. Energy facilities, ports, communication networks, transportation systems, and other essential infrastructure are increasingly exposed to drone-enabled sabotage, particularly as autonomous aerial and maritime systems become more capable and accessible. The ability of relatively low-cost platforms to threaten high-value assets creates a significant strategic and economic imbalance, challenging traditional approaches to deterrence and defense.

Looking ahead, advances in artificial intelligence, drone swarms, autonomous targeting, and additive manufacturing are likely to further expand terrorist capabilities. The increasing integration of advanced sensors, autonomous navigation, and locally produced components will make drones more difficult to detect and defeat. For NATO, addressing this evolving threat will require continuous technological adaptation, investment in layered counter-UAS systems, intelligence sharing, and innovative approaches to defense planning.

In chapter seven, "Terrorist Recruitment and Online Social Engineering: Technology, Innovation and Future Global Trends," Professor Richard Aldrich argues that the digital revolution has transformed not only the tools available to terrorist organizations but also the broader dynamics of recruitment, radicalization, financing, and organizational innovation. As the once-celebrated Silicon Valley ethos of 'move fast and break things' has reshaped the global information environment, digital

technologies have accelerated the speed, scale, and disruptive potential of terrorist activity while simultaneously weakening traditional state authority -- blurring the boundaries between previously distinct forms of extremism.

The chapter contends that technological innovation has fundamentally altered the terrorist recruitment ecosystem. Social media platforms, encrypted messaging applications, the dark web, and increasingly generative artificial intelligence enable extremist organizations to identify, influence, recruit, and mobilize individuals with unprecedented precision and global reach. These technologies are not merely communication tools; they integrate recruitment with propaganda, operational planning, financing, and command and control, creating a digitally enabled terrorist ecosystem. While many attacks continue to rely on relatively low-technology tactics, their preparation, coordination, financing, and amplification are becoming increasingly digital.

The author emphasizes that one of the chapter's most significant insights is that the greatest impact of digital transformation is cultural rather than technological. He argues that "the most alarming aspect of terrorists embracing digital technology is cultural change, since it encourages new kinds of participants to innovate in a realm where, historically, change has been slow." He suggests that creative terrorist groups are dangerous because of their potential to inflict surprise.

Digital ecosystems lower barriers to participation, accelerate experimentation, and foster continuous innovation within extremist networks. This is particularly evident among emerging violent extremist movements, including the extreme right, whose online communities rapidly adapt new technologies and tactics. The resulting capacity for rapid adaptation and strategic surprise represents one of the defining characteristics of terrorism in the coming decades. As innovation becomes decentralized and increasingly driven by digitally connected individuals rather than hierarchical organizations, the future terrorist threat will be shaped less by technological sophistication alone than by the ability of terrorist actors to exploit emerging technologies creatively and unexpectedly raising the stake of being able to predict or mitigate future attacks.

Dr. Lewis Herrington, in his chapter entitled, "Future Terrorism, Extremism, and the Rise of Single-Issue Ideologies: Strategic Lessons from Ontological Security," argues that future terrorism will be driven less by cohesive ideological movements than by atomized extremism, single-issue grievances, and digitally accelerated radicalization. He contends that emerging forms of extremism—including right-wing, far-left, anti-state, and technology-related movements—exploit a growing crisis of ontological security, in which individuals experience diminished belonging, agency, and meaning. While ontological insecurity does not itself produce terrorism, it can increase susceptibility to extremist narratives when combined with social isolation,

identity fusion, perceived grievance, and digitally mediated echo chambers. Digital platforms amplify these dynamics by creating synthetic communities, reinforcing polarization, and transforming political grievances into uncompromising moral causes, while also providing opportunities for hostile states to exploit societal divisions through cognitive warfare and disinformation. Herrington maintains that effective counterterrorism must extend beyond intelligence and law enforcement to address the underlying social and psychological conditions that facilitate this type of radicalization.

In chapter nine, titled “Online Intervention Strategies for Preventing Youth Radicalization,” Dr. Erin Saltman examines how advances in digital technologies are reshaping both youth radicalization and the strategies designed to prevent it. As younger generations become increasingly immersed in personalized online environments, digital platforms have become central spaces for identity formation, community building, and psychosocial support. These same environments, however, have also become fertile ground for extremist recruitment, contributing to a rise in youth radicalization and lone-actor terrorism across diverse ideological movements.

At the same time her chapter argues that the rapid evolution of online platforms is driving parallel innovation in the prevention space. Technology companies are increasingly deploying hybrid moderation systems that combine artificial intelligence, behavioural analytics, and predictive risk models to identify and disrupt extremist activity at scale. While these capabilities offer significant opportunities for earlier intervention, they also raise complex ethical questions relating to privacy, algorithmic bias, transparency, and the protection of civil liberties.

In chapter ten, “Strategic Foresight and Counter-Terrorism Futures: Aligning NATO Doctrine with Emerging Threats and Structural Drivers,” Dr. Gergely Németh assesses the future of counterterrorism through the lens of NATO doctrine and strategic foresight. Drawing on NATO's *Strategic Concept 2022*, *Allied Joint Publication-01 (AJP-01)*, the *2024 Policy Guidelines on Counter-Terrorism*, and the institutional role of the Defence Against Terrorism Centre of Excellence, he evaluates the Alliance's preparedness against the long-term trends identified in *Strategic Foresight Analysis 2023*.

Dr. Németh argues that disruptive technologies, climate change, resource scarcity, and the growing influence of empowered non-state networks will fundamentally reshape the character of terrorism and the requirements for Allied responses. Among the futures examined, the scenario of pervasive strategic competition is assessed as the most likely, requiring NATO to adopt an integrated, multi-domain counterterrorism posture that simultaneously addresses the cognitive, cyber, and physical dimensions of the threat. The current NATO doctrine contains important gaps, particularly in its treatment of technologically empowered non-state actors, the governance of emerging technologies, the climate-security nexus, and the

convergence of terrorism with hybrid warfare. Addressing these shortcomings will be essential if NATO is to maintain an effective counterterrorism posture in an increasingly complex strategic environment.

Taken together, the chapters demonstrate that effectively addressing the evolving challenges posed by terrorism in the future requires not only an understanding of the diverse forms these threats may assume, but also careful consideration of how terrorist actors may exploit cross-domain threat enablers. These enablers, outlined below, have the potential to amplify existing vulnerabilities and facilitate the convergence of different forms of terrorist activity across domains.

Cross-Domain Threat Enablers

Enablers	Types of Modus Operandi
Artificial Intelligence	planning, reconnaissance, autonomous operations, deepfakes, cyber attacks, social engineering, autonomous systems
Commercial Drones	intelligence collection, kinetic attacks, delivery of explosives, electronic warfare, aerial/UAS operations, maritime or surface operations, subsea/UUV operations, ground/UGV operations, space operations
Organized Crime Networks	financing, logistics, weapons procurement, document fraud, smuggling, money laundering
Cryptocurrency & Digital Finance	fundraising, sanctions evasion, anonymous transfers, criminal partnerships
Social Media and Gaming Platforms	recruitment, radicalization, propaganda, operational communications, influence operations
Encrypted Communications	secure command and control, operational security, decentralized organization
Commercial Satellite Networks	global connectivity, communications resilience, remote operations
Subsea Cables and Digital Infrastructures, Low Earth Orbiting Satellites (LEOs)	strategic targets whose disruption creates cascading economic and communication effects
Critical Infrastructure Interdependence	enables cascading failures across energy, communications, finance, transportation, healthcare, and government services

Artificial intelligence, autonomous systems, commercial satellite constellations, cyber capabilities, encrypted communications, digital finance, biotechnology, and unmanned platforms have dramatically lowered the barriers to acquiring capabilities that, only two decades ago, were the preserve of nation-states. At the same time, global supply chains, subsea communications cables, maritime trade routes, cloud computing, and critical digital infrastructure have created new strategic vulnerabilities that terrorists can exploit to achieve effects far beyond the physical destruction they inflict.

Consequently, terrorism in 2040 is unlikely to be confined to a single domain. Instead, future terrorist campaigns are likely to be conceived and executed as multi-domain operations that combine physical violence with cyber disruption, information manipulation, electronic interference, and attacks on critical infrastructure. Terrorist organizations have long demonstrated proficiency in operating on land and in cyberspace, but they are increasingly expanding their capabilities into the air and maritime domains through the use of autonomous drones. Many of the commercially available drone technologies are dual-use and can be adapted for hostile purposes. Equally significant is their growing ability to operate within the cognitive domain, where artificial intelligence, algorithmically amplified propaganda, deepfakes, and highly personalized social engineering can shape public perceptions, recruit supporters, and undermine trust in institutions long before any physical attack occurs.

A future terrorist campaign may therefore unfold across multiple domains simultaneously. An operation might begin with an artificial intelligence-generated influence campaign designed to polarize public opinion and recruit sympathizers. This could be followed by a cyberattack against the management systems of a major port, electromagnetic interference that disrupts GPS and emergency communications, autonomous explosive surface vessels targeting commercial shipping, coordinated drone swarms overwhelming security forces, and simultaneous acts of sabotage or mass-casualty attacks on land. None of these activities would occur in isolation; together they would constitute a coordinated campaign intended to produce cascading political, economic, and psychological consequences that extend far beyond the immediate attack.

Feasible Attack Scenarios Across Domains

Domain	Primary Terrorist Objectives	Representative Threats	Emerging 2040 Capabilites	Primary Targets
Land	cause casualties, disrupt	bombings, shootings,	autonomous ground robots, AI-	cities, government buildings,

	governance, create fear	hostage-taking, CBRN attacks, infrastructure sabotage, assassination, sabotage of transport Aircraft attacks, MANPADS, drone attacks, UAV swarms, airborne IEDs	assisted planning, smart explosives, 3D-printed weapons, swarming systems	transport hubs, critical infrastructure, public events
Air	attack aviation, bypass borders, strike strategic targets	aircraft attacks, MANPADS, drone attacks, UAV swarms, airborne IEDs	autonomous drone swarms, AI navigation, long-range UAVs, cargo drone exploitation	airports, aircraft, government facilities, energy infrastructure, nuclear infrastructure, public gatherings
Maritime	disrupt global trade and energy flows	Piracy alliances, port attacks, mining, attacks on shipping, underwater sabotage, attacks on choke points, main trade routes	USVs, UUVs, underwater drones, autonomous explosive boats, AI navigation	ports, shipping lanes, offshore platforms, LNG terminals, subsea infrastructure
Space	disrupt communications navigation, intelligence	interference with satellite services, exploitation of commercial satellite networks	jamming, spoofing, cyber attacks on satellite control systems, exploitation of mega-constellations	LEO satellites, satellite communications, GPS/GNSS, space-based internet services
Cyber	disrupt essential services and	ransomware, destructive	AI-generated malware,	power grids, banking,

	undermine confidence	malware, cyber-enabled terrorism, critical infrastructure attacks	autonomous cyber agents, quantum-enabled attacks (future), supply-chain compromises	hospitals, telecommunications, transportation, government networks
Electromagnetic (EMS)	deny communications and sensing	GPS jamming, RF interference, communications disruption, spoofing	portable EW systems, AI-controlled jamming, commercial SDR exploitation, drone-enabled EW	emergency services, military communications, aviation, shipping, critical infrastructure
Cognitive / Information	influence behaviour, polarize societies, recruit supporters	propaganda, online radicalization, deepfakes, disinformation, psychological operations, intimidation	generative AI, synthetic media, personalized influence campaigns, social engineering at scale, automated bot networks	public opinion, elections, social cohesion, government legitimacy, vulnerable individuals

In the future terrorism will not be defined by a single act or actor; it will instead be representative of a fluid ecosystem of multiple actors and multiple types of modus operandi. Terrorist groups increasingly borrow methods from organized crime, exploit commercial innovation, leverage geopolitical rivalries, and weaponize the openness of democratic societies. They do not need to defeat states conventionally. Instead, they seek to impose disproportionate political, economic, and psychological costs through carefully selected acts of disruption. In an era of hyperconnectivity, even modest attacks can cascade through financial systems, transportation networks, information ecosystems, and public confidence, creating strategic effects far beyond their physical scale.

This evolution challenges many of the assumptions that have shaped counterterrorism since the attacks of the early twenty-first century. Success can no longer be measured solely by disrupted plots, arrested operatives, or degraded

organizations. Future terrorist threats are likely to emerge from decentralized networks that assemble rapidly, exploit globally using available technologies, and dissolve before traditional intelligence and law enforcement mechanisms can respond. The distinction between physical and digital attacks will continue to blur, while campaigns increasingly combine cyber operations, disinformation, economic disruption, sabotage, and kinetic violence into a single coordinated strategy.

As the distinction between conflict, war, crime, and terrorism continues to blur, counterterrorism can no longer be viewed solely as a law enforcement or intelligence function. It must instead become an integral component of national resilience and multi-domain defense. The defining challenge of 2040 will not simply be defined by preventing terrorist attacks, but by anticipating and countering increasingly sophisticated campaigns designed to exploit the interconnected nature of modern societies and the evolving dynamics of global power.

Another recurring theme throughout this book has been that the future battlespace extends far beyond traditional security institutions. Technology companies increasingly shape the information environment in which extremist narratives spread or fail. Telecommunications providers and satellite operators maintain infrastructure upon which both societies and adversaries depend. Shipping companies, financial institutions, cloud providers, artificial intelligence developers, and operators of critical infrastructure all occupy positions on the front line of national security. The defense of society against terrorism is therefore becoming a genuinely whole-of-society and whole-of-government endeavor, requiring unprecedented collaboration between governments, military, industry, private investors, academia, and civil society.

In the past, technological innovation was always regarded as the key to protecting states against nefarious actors. Yet technology alone will neither determine victory nor guarantee security. Every technological advance that strengthens resilience also creates new vulnerabilities to exploit. Artificial intelligence may improve threat detection while simultaneously enabling more persuasive disinformation and autonomous attack capabilities. Drone defenses will evolve alongside increasingly intelligent autonomous systems. Quantum technologies, synthetic biology, and future communications networks will each present similar cycles of innovation and adaptation. The decisive advantage will belong not to those possessing the most advanced technologies, but to those capable of adapting institutions, legal frameworks, partnerships, and strategic thinking faster than their adversaries.

The challenge, therefore, is not to predict every future terrorist innovation with precision. History demonstrates that adversaries will continue to surprise even the most sophisticated intelligence communities. Rather, the objective must be to build

systems that are resilient, adaptive, and capable of responding effectively to unforeseen forms of asymmetric warfare.

The question facing policymakers and military planners is no longer whether terrorism will evolve. It will. The more important question is whether democratic societies can evolve more rapidly than the threats they confront. The answer will depend not only on intelligence and military power, but on governance, innovation, international cooperation, and the preservation of the very values that terrorism seeks to undermine.

The balance of power is being rewritten not only by divisions as regards globalism and nationalism but by innovation itself — a technological order that redefines human potential. Who can innovate the fastest will design and determine the future. Perhaps not only chief innovating countries will drive innovation but perhaps AI itself -- who will ultimately be in control? Nations, industries, and individuals alike are reshaping their strategies to adapt to this shifting landscape, where data, algorithms, and sustainability are the new currencies of influence and power.

NATO has a powerful hand to play as emerging markets make generational policy, partnership and investment decisions for advanced digital infrastructure and services that have the potential to impact global security for generations to come. It is therefore important that NATO ensures that most vital tech companies remain close to their orbit. It will also be important to ensure that a good portion of the global technological ecosystems will remain rooted in democratic values and shared values of openness, freedom and rule of law. Failure to support these strategic alliances, could lead to a global technological world order that is no longer vigilant in keeping terrorists or criminal actors from abusing technology for nefarious purposes.

In 2040, conflicts will be fought across cyber and cognitive domains as much as physical territories and maritime spaces, through information as much as firepower, and within societies as much as between states. Preparing for that reality begins with recognizing terrorism for what it has become: not an anomaly within international security, but one of the defining modes of warfare of the twenty-first century. In a world characterized by accelerating technological change and persistent geopolitical instability, resilience may become the most important national security capability of all.

Centre of Excellence Defence Against Terrorism

COE-DAT



Scan to reach the products of COE-DAT

www.coedat.nato.int