07/10/2025

IN FOCUS

Enhancing Cognitive Security and Societal Resilience to Counter Cognitive Warfare

Driven by geopolitical tensions and rapidly evolving technological developments, forms of cognitive warfare and hybrid threats have intensified, targeting the individual citizen and making today's information ecosystem increasingly difficult to navigate. In addition to defending against such attacks, the ability to deter such threats and protect information and cognitive integrity requires a whole-of-society approach that supports citizens and strengthens societal resilience by enhancing cognitive security through a combination of societal, educational, technical, policy and regulatory measures.

Dr Jean-Marc Rickli
Head of Global and Emerging Risks and
Director of the Polymath Initiative, GCSP

Mr Tobias Knappe
Project and Research Officer,
Polymath Initiative, GCSP

On 6 December 2024, in an unprecedented decision, Romania's constitutional court annulled the results of the country's presidential election and called for a new vote. This followed the surprise win of the little-known far-right candidate Călin Georgescu in the first election round on 24 November. Declassified Romanian intelligence described aggressive hybrid actions during the election campaign that suggested Russian interference in the electoral process. While the Russian government denies involvement, Georgescu's sudden rise was reportedly driven by artificial accounts and content on platforms such as TikTok, most of which originated from Russia-affiliated actors and networks. Moldova's recent parliamentary elections have witnessed similar interference. This meddling with the electoral process of, respectively, a NATO and European Union (EU) member and an aspiring EU member state in times of increasing geopolitical tensions exemplifies how disinformation undermines political unity, contributes to polarisation, and targets civil society.

Challenges to the global information ecosystem

Today's global information ecosystem is highly digital, fast-paced, and increasingly complex. The Romanian and Moldovan cases demonstrate the vulnerability of open societies – a core feature of any democracy – to hybrid tactics in the digital space, the difficulty of attributing information manipulation operations, and the complexity of addressing such threats without undermining democratic processes. They are part of broader challenges facing the current global information ecosystem that include increasing threats from disinformation and artificial intelligence (AI)-driven influence campaigns that citizens find increasingly difficult to navigate. While disinformation is not a new phenomenon, its scale, reach, persistence and sophistication have grown rapidly. The availability of technologies such as generative or agentic AI advances the creation, spread, and amplification of disinformation at unprecedented levels and increasingly allows for the personalised targeting of individuals. While deepfake content has risen tenfold globally over the past year, the average person now encounters over ten online scams daily, including around three deepfake videos. These risks undermine information integrity and pose particular risks to democracies and open societies.

With geopolitical tensions increasing, forms of aggression that remain below the threshold of armed conflict have intensified, including both hybrid warfare, which blends conventional and unconventional methods, and grey-zone tactics. Developments in cognitive AI and neurotechnologies are dramatically increasing the ability to profile individuals, which in turn enhances opportunities to conduct cognitive warfare that aims to influence an opponent's reasoning and decision-making. These actions often blur the lines between civilian and military domains and target citizens at the individual level – and, most importantly, make the brain, via the cognitive

domain, a new dimension of warfare. Despite the omnipresence of hybrid threats, citizens are ill-equipped to navigate today's information eco-system shaped by disinformation and cognitive operations, and current efforts to protect information integrity are insufficient.

Cognitive security as a response to hybrid warfare

Open societies must find ways to protect the information space without compromising the principles on which they rest. A proactive approach to mitigating such threats is through deterrence. There are two main forms of deterrence: deterrence by punishment, involving the threat of severe punishment if an attack occurs, and deterrence by denial, which seeks to deter an action by making it unfeasible or unlikely to succeed. The former can include potential retaliation operations, public exposure, or the promotion of competing narratives among an adversary's population.

Due to the inherent ability of cognitive warfare to affect or influence the civilian domain, effective deterrence also implies denying an adversary their ability to influence one's own society by strengthening societal resilience. This refers to a community's proactive nature, preparedness, and the willingness of people to act in critical situations, withstand shocks and disruptions, recover, adapt, and continue their lives. An important component of societal resilience in the era of cognitive warfare is the notion of cognitive security, a state and process in which undesired malign influence or manipulation is incapable of altering human cognition. To achieve this, the main instruments are mostly non-military and include, among others, education, information literacy and critical thinking, technical tools for verified information, support to quality journalism, and responsible innovation. If societal resilience is enhanced, cognitive manipulation becomes less effective, which in turn increases deterrence by denial. Cognitive security therefore forms a critical pillar of this response.

How to enhance cognitive security

Defending against threats to cognitive security requires a multifaceted approach that combines societal, educational, technical, policy and regulatory measures. We can identify at least four measures that contribute to increase societal resilience. Firstly, a mindset shift towards resilience can help defend against cognitive threats by raising awareness among the broader public. The Swedish government's "Don't Be Fooled" handbook seeks to inform citizens of any age on how to be better protect themselves against disinformation, and actively involves the population in psychological defence through tools such as the informed triangulation of sources.

Secondly, formal education has an important role to play in fighting disinformation by fostering critical thinking and focusing on the human element of resilience. A recent study has demonstrated that it can take as little as three minutes of sensitisation training for signs of its effectiveness to appear. Finland's approach of teaching children about disinformation from primary school onwards has led to improved capabilities to find, assess and safely handle information found online. Together with a mindset shift towards resilience, such proactive and systematic educational initiatives to promote information literacy among a population – including in the areas of media, digital, and AI literacy – contribute to enhancing cognitive security in times when the majority of young people primarily or exclusively consume news via digital channels instead of traditional media sources. Yet measures like these have yet to be adopted in many countries.

Thirdly, technical solutions and an innovation ecosystem that rewards transparency and safety-by-design rather than black box approaches to technological development have an important role to play in the long term. One example of such a responsible use of digital technology is the Taiwanese open-source platform Polis, which enables productive civil engagement and an inclusive approach to legislation rather than fuelling polarisation to gain engagement. This approach contributes to Taiwan's position as a leader in digital democracy and helped it to counter Chinese disinformation in its 2024 election.

Fourthly, policy and regulatory responses are required to protect people's privacy and counter the potential weaponisation of emerging technologies. For instance, questions around neurorights, which can be defined as the ethical, legal, social, or natural principles of freedom or entitlement related to a person's cerebral and mental domain, are also becoming increasingly prevalent, especially to deal with neurotechnological advances such as brain-computer interfaces or the increasing availability of EEG consumer-grade headsets and research-grade devices with the ability to detect detailed brain signals.

Conclusion

Information has always been used as a form of weapon in warfare, but current technological developments magnify its impact by dramatically reducing the costs of subverting populations. As such, its misuse should be seen as a new kind of WMD: not a weapon of mass *destruction*, but of mass *disinformation* designed to target citizens' information and cognitive integrity. The best way to counter this new type of warfare – cognitive warfare – besides actively defending against it, is through a whole-of-society approach that helps citizens in a variety of ways to navigate an informational space full of disinformation and AI-generated content. Enhancing cognitive security by focusing on the human element of resilience and promoting other appropriate measures contributes to protecting open societies and strengthening societal and democratic resilience. Governments have a responsibility to support the required infrastructure and guarantee conditions that make a society more resilient and create the framework conditions for citizens to form fact-based opinions. Adopting a proactive, human-centred approach and implementing a combination of appropriate cognitive security measures will contribute to making citizens, institutions, and elections more resilient and hence reinforce the foundations of open societies.

Geneva Centre for Security Policy

www.gcsp.ch/publications
info@gcsp.ch