Algorithmic North: Weather, Security and International Law

Amanda H. Lynch and Charles H. Norchi

November 2025

GCSP Policy Brief No.21

GCSP
Geneva Centre for Security Policy

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 55 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

The GCSP Policy Briefs Series

The GCSP Policy Briefs series addresses current security issues, deduces policy implications and proposes policy recommendations. It aims to directly inform policy- and decision-making of states, international organisations and the private sector.

Under the leadership of Ambassador Thomas Greminger, Executive Director of the GCSP, the series is edited by Professor Nayef Al-Rodhan, Director of the Geopolitics and Global Futures Department, and Doctor Tobias Vestner, Director of the Research and Policy Advice Department & Head of Security and Law, and managed by Ms Christine Garnier Simon, Administration and Coordination Manager, GCSP Geopolitics and Global Futures.

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-440-0

About the authors

Amanda H. Lynch is an atmospheric scientist and climate modeler. She serves as the Lindemann Distinguished Professor at the Department of Earth, Environmental and Planetary Sciences of Brown University. Her research comprises three books and over 130 research articles and book chapters, concerns the intersection of science and policy, with a focus on the Arctic as a place that expresses convergences of rapid change in natural and human systems. She has collaborated with a range of stakeholders and community partners, including Iñupiat, Sakha and Yorta Yorta Indigenous Peoples. Lynch won the Priestly Medal in 2008 and the Myres S. McDougal Prize in International Law in 2022, and is a Fellow of the American Meteorological Society, the Australian Academy of Technological Sciences and Engineering, and the Norwegian Scientific Academy for Polar Research. At the UN World Meteorological Organization, Lynch chairs the Research Board and co-chairs the Joint Advisory Board on AI.

Charles H. Norchi is the Benjamin Thompson Professor of Law in the University of Maine School of Law where he is Director of the Center for Oceans Law and Founder of the Arctic Law Program. He is an expert in International Security and International Maritime & International Law, about which he is widely published and has lectured in forty-four countries. Norchi is co-chair of the International Institute for Law, Science and Policy in Geneva. Professor Norchi is a Fellow of the Explorers Club, the World Academy of Arts and Sciences, and the Royal Asiatic Society of Great Britain and Ireland (RAS) for which he is the namesake of the RAS Afghanistan prize. He has worked as a journalist in Afghanistan, legal counsel to UN organizations and international companies, has studied in France and Switzerland, and holds degrees from Harvard University, Case Western Reserve University School of Law and Yale Law School.

Introduction

Artificial intelligence (AI) and machine learning (ML) technologies[1] are reshaping core practices and infrastructure worldwide, but in the Arctic, this transformation is not merely disruptive – it is decisive. The region is at once climatically unstable, geopolitically contested and operationally fragile. Accurate weather, water, and climate (WWC) services[2] form the backbone of safety, mobility, and sovereignty in the High North.[3] As Arctic stakeholders turn increasingly to AI/ML to enhance decision-making support, they are rapidly building dependencies on systems in an institutional vacuum. In a region where the margin for error is slim and the consequences of failure severe, these shifts demand urgent policy attention. At the same time, international law is struggling to keep pace. No treaty regime governs algorithmic decision-making in the Arctic, and the patchwork of relevant norms were not designed for this convergence of technical innovation, commercial incentives, and environmental exigency. This Policy Brief situates the algorithmic transformation of Arctic WWC services within its broader legal and security context. It concludes by outlining three domains for policy intervention: international organisations, international law and international security.

[1] An algorithm is a precise set of instructions that guide a computer through steps to solve a problem. AI and ML approaches comprise algorithmic techniques that learn temporal and spatial relationships between and within the continuous stream of observations, turning them into forecasts, risk indicators, and operational advice. Unlike rule-based algorithms, these data-trained models refine themselves as new information flows through the cycle (see Annex, Table 1).

[2] The WWC value cycle denotes the integrated suite of observational, modelling, and advisory services that national meteorological and hydrological agencies, research institutes, and private vendors provide, both in the public interest and as commercial products. These products are interoperable across nations, networks and computer systems by virtue of the Convention of the World Meteorological Organization.

[3] Formally, the Arctic or High North comprises the regions north of 66o33'N latitude. However, regions with Arctic characteristics also include terrestrial regions somewhat south of this line.

The weather, water and climate value cycle

In the Arctic, accurate forecasts and timely warnings are indispensable for safeguarding human life, enabling secure military and civilian operations, supporting fisheries and industry, and ensuring the resilience of critical infrastructure in an environment where small errors can have outsized consequences. Even with satellites sweeping the skies, the physics of the problem still demands on-the-ground information, but no one country's observations can see the whole picture. The atmosphere knows no borders. Indeed, the physics of the problem is such that each nation's weather data is more valuable to others than to itself, making international cooperation the only way global forecasting can function. In the international system, this cooperation is governed by a number of organisations, with the first among them being the World Meteorological Organization (WMO), as well as a web of international legal instruments and state practices. The new science of AI is now embedded in this complex domain.

AI-/ML-based technologies are no longer laboratory curiosities, and the Arctic is no exception. In an almost unprecedentedly dynamic research and development environment, AI/ML approaches are rapidly permeating every link of the WWC value cycle – from satellite tasking and autonomous ocean profilers to real-time forecast fusion and decision dashboards. These approaches (see Annex, Table 1) are not typically based on large language models, except in specific applications associated with translating a forecast into a plain-text or visual communication to an end user. The revolutions in weather analysis, forecasts and services constitute a different category – not a promise of general intelligence, but targeted algorithms that are quickly improving on traditional methods. In the High North, where sensors are sparse, logistics perilous, and environmental change unprecedentedly swift, the turn toward machine learning is both inevitable and transformative. This algorithmic turn, however, arrives at a geopolitical moment in which safety, sovereignty, sustainability and strategic competition intersect more sharply than at any time since the Cold War.

The Arctic exemplifies the interconnectedness of the WWC value cycle. Data flow begins with polar-orbiting satellites and Global Navigation Satellite System (GNSS) soundings, along with terrestrial, shipborne and aerial sensors, and through data assimilation processes passes through forecast models to terminate in forecast products, which are then delivered through a variety of channels. Relative to lower latitudes, the Arctic is characterised by sparse and dirty data, and the ice phase presents additional complexity. Analysis of forecast skill and diagnoses of forecast "busts" (where the model guidance deviates so badly from the observed evolution that standard skill scores collapse and post-event reviews are triggered) in turn feed back to design choices at every stage, creating a cycle. And every stage is implicated in overlapping sovereignty and jurisdictional claims: states invoke the Law of the Sea to regulate sensors in their maritime zones; airspace is subject to the UN Convention on International

Civil Aviation (Chicago Convention); space-based instruments remain under the "continuing supervision" of launching states; and terrestrial weather stations are governed domestically, but subject to technical standards set by the WMO and other international organisations. This complex of systems, grounded in agreements supporting free data sharing and interoperability under the Convention of the World Meteorological Organization, creates multiple points of friction where geopolitical interests collide with operational imperatives.

As sea-ice retreat promises year-round navigability and accelerated resource exploration, Arctic stakeholders are racing to harness AI/ML for ice-edge prediction, maritime routing, climate-risk attribution, and critical-infrastructure defence. Yet the same tools that promise granular foresight also destabilise long-settled legal equilibriums: Who owns data harvested in another state's exclusive economic zone? May proprietary diffusion models satisfy the International Convention for the Safety of Life at Sea (SOLAS) and the International Maritime Organization Polar Code requirements when their inner workings are inscrutable? How does indigenous data sovereignty under the United Nations Declaration on the Rights of Indigenous People principle of "free, prior and informed consent" coexist with the WMO's standard of "free and unrestricted exchange"?

Against this backdrop, this Policy Brief maps the emerging AI/ML landscape across Arctic WWC services and interrogates its legal implications. These include the tensions among WMO sharing norms, claims under the United Nations Convention on the Law of the Sea (UNCLOS), and CARE[4]-based Indigenous control; questions of liability for closed-source forecasts;[5] private-sector consolidation; human-rights safeguards; and information security. It closes by outlining the policy developments needed to reconcile innovation with equity and environmental stewardship before de facto norms ossify.

In short, we seek to illuminate how law must evolve if AI/ML is to fortify rather than fracture the Arctic's rapidly shifting weather, water and climate frontier. We urge policy imperatives – to anticipate governance gaps now, thus enabling states and stakeholders to harness the AI/ML revolution toward enhancing polar safety and international security. An alternative future – allowing opaque algorithms to erode Arctic security and degrade the legal order by default – would be calamitous. If one plausible future is algocracy, it could begin in the High North, with weather.

[4] CARE principles for indigenous data governance – collective benefit, authority to control, responsibility, ethics – are intended to complement FAIR (findable, accessible, interoperable, reusable) data standards.

[5] A "black box" system is one whose inputs and outputs are visible, but whose inner workings remain hidden. A "closed-source" system refers more specifically to software or models whose underlying code, data, or design is proprietary and not publicly accessible, meaning users can operate them, but cannot freely inspect, modify, or redistribute them. An "open-source" system, by contrast, makes the code or model architecture available for public use and modification, although in AI/ML this can range from full transparency (code and training data) to partial openness, such as sharing model weights without the data or methods used to produce them.

Data and authority in the WWC value cycle

The development of AI/ML approaches in the High North – as elsewhere across the globe – requires a massive and continuous stream of data. This data encompasses modes of observation from satellite constellations to local observations, yet each mode is governed by distinct legal regimes. Space-borne sensors operate under domestic remote-sensing licences and Outer Space Treaty Article VI "continuing supervision". Marine vessels and platforms require coastal-state consent under UNCLOS and flag-state oversight. Unmanned aerial vehicles and manned aircraft fall under the Chicago Convention. Ground-based weather stations are a purely domestic concern until their data is fed into the WMO Information System (WIS.) Community-collected and some research data invokes CARE-based indigenous sovereignty. This complex of data streams is governed by standards set by agencies such as the International Telecommunication Union and the International Organization for Standardization, which are characterised by self-interested compliance. These regimes create a three-tier gradient of accessibility:

i. the open core of essential and compliant WWC observations shared freely through the WIS to other national meteorological and hydrological services, but not always more widely;

ii. licensed augmentation streams – high-resolution satellite imagery or proprietary buoy feeds – guarded by subscription contracts; and

iii. datasets released only through benefit-sharing or other agreements.

Ideally, AI pipelines entering this complex should therefore embed robust provenance tags and licence checks against proprietary, sovereign or ethical constraints. Harmonising remote-sensing licences, polar-orbit launch deals and sensor charters with "open-by-design" clauses, for example, is a significant ongoing challenge.

A key issue is authority in this new regime of hybrid closed- and open-source systems and data. The Arctic WWC value cycle now depends on two very different kinds of actors. Firstly, public good providers include national meteorological and hydrological services, intergovernmental organisations, and publicly funded research centres. These providers are funded by domestic legislation and international agreements to supply open-forecast products. They operate largely under the WMO Unified Data Policy, although compliance is variable, and in the Arctic are subject to the relevant state agreements, including SOLAS and the Polar Code. Based on WMO surveys of its members, only around one-third of these providers are designated as the exclusive authoritative voice for all hydrometeorological hazards. Of the remainder, some are considered official sources, but not the sole authority (including multi-agency warning architectures), and around a quarter have no statutory mandate. All public good providers are incentivised to maximise transparency in order to maintain public trust and ensure compliance with international agreements.

Commercial providers include private firms offering subscription application programming interfaces, vessel-routing dashboards or bespoke AI/ML models, and are governed by contract law. These vendors are subject variously to product-liability, consumer protection and professional negligence doctrines that vary from state to state. While there is typically no immunity from these, there is greater freedom to restrict data, neural weights (settings for AI/ML algorithms) or the algorithms themselves as commercial-in-confidence.[6] Commercial providers are incentivised to protect intellectual property, recoup research and development costs, and expand their customer base. These incentives can have the unintended effect of reducing explainability and widening information asymmetries.

A specific concern in the Arctic is that coastal and flag states must ensure "adequate and effective" meteorological information (SOLAS, chap. V, reg. 5; Polar Code, part I-A, sec. 11). In the case of a forecast bust,[7] public provider liability is channelled through domestic public law. In cross-transnational situations, technical staff exchanges or perhaps diplomatic engagement rather than tort litigation is the usual path. Private providers do not fall under these regimes. Courts are increasingly analogising forecast services to "products" such that strict liability or negligence claims may attach. That said, limiting clauses are unlikely to defeat mandatory SOLAS and Polar Code safety standards.

Security and weather in the Arctic

Weather in the Arctic is inseparable from security, and indeed ice and storms have not shielded the Arctic from the effects of the international system. The region is subject to the power and interests of states and other actors across land, sea, air, and outer space. Freedom of navigation patrols, submarine surveillance, strategic aviation, and communications networks all depend on reliable forecasts and warnings. When things inevitably go wrong, search-and-rescue missions also require continuous access to meteorological services. In this environment, the forecast is not an auxiliary product, but a critical enabler of defence posture, force mobility and situational awareness. When prediction falters, risks to assets and personnel escalate and the credibility of deterrence itself can erode.

For security actors, the legal stakes are high. Obligations under SOLAS require vessels, including naval auxiliaries and icebreakers, to be equipped to receive, access, and use "adequate and effective" meteorological information. The Polar Code reinforces this for the Arctic by requiring that vessels demonstrate in their *Polar Water Operational Manual* that they have reliable means of obtaining and applying relevant meteorological and ice information. If forecasts prove

[6] "Commercial-in-confidence" refers to business-sensitive information that is considered private and not for public disclosure due to its potential to damage a company's competitive position.

[7] A "forecast bust" is a poor weather forecast when the actual weather turns out significantly different from what was predicted.

unreliable – because data has been withheld or because closed-source or proprietary models provide limited explainability – the resulting gaps may compromise compliance with these international safety regimes. In practice, states resolve such disputes diplomatically, but as AI systems displace traditional models and private sector offerings supplement authoritative government sources, questions of liability and attribution become more relevant. When a closed-source algorithm misses a polar cyclone that damages strategic assets, who bears responsibility – the state that operated the platform, the vendor that trained the model or the commander who relied on it?

The ways in which the principles of open-source and open data are flexibly applied in hybrid public-private systems further complicate the landscape. Large and small technology firms now provide high-quality forecasting capacity, data hosting and model-training services that are embedded in security operations. Yet these providers are answerable primarily to shareholders, not to international law or domestic authorities. Export controls, commercial disputes, or strategic realignments can restrict access to essential data streams or neural weights, having the potential to degrade the forecast cycle on which military actors depend. States risk entanglement in vendor lock-in, where operational security becomes contingent on the commercial priorities of firms beyond the purview of existing treaties.

Cyber threats can pierce nearly any security envelope. It has already been established that the jamming and spoofing of data and navigation signals can disable autonomous vessels or distort atmospheric soundings, but in AI/ML systems, model-poisoning attacks can insert subtle errors into training corpora[8]. These vulnerabilities expose the critical infrastructure of WWC services whose disruption could alter the strategic balance. Existing instruments such as the Polar Code or bilateral search-and-rescue compacts do not yet account for this cyber-physical dimension.

The convergence of these dynamics highlights an urgent legal problem: the Arctic security architecture is likely to become dependent on forecasting systems that straddle public and private domains, but effective law lags. In the end, the strategic value of weather services in the Arctic lies not only in their technical accuracy, but in the stability of the legal order that underpins them. While international law does not eliminate competition among states, it can channel conflicting demands into forms that preserve safety and predictability. Without proactive adaptation, the risk is clear: forecasting infrastructure could become weaponised through the denial of data, cyber interference or proprietary withdrawal, undermining both the collective security and public order of the Arctic.

[8] Training corpora refers to the large collections of text, data, or images used to teach an artificial intelligence system to recognize patterns, make predictions, or generate responses.

Lex specialis or constitutive process?

International law facilitates patterns of authority and control that purport to impose stability, predictability, and continuity in an otherwise unorganised global arena. The Arctic WWC value cycle relies on a data chain whose every link is entangled in overlapping sovereignty, sharing, and privacy regimes underpinned by international law – the authoritative decisions of the world community expressed in conventions and custom. It supplies the scaffolding for these vital services. Unlike Antarctica, there is no dedicated treaty regime for the Arctic; instead, the region is governed by generally applicable and certain specialised legal instruments. As a general matter, the international law that applies to other regions of the world is equally applicable to the Arctic. States are under an obligation to refrain "from the threat or use of force against the territorial integrity or political independence of any state" (UN Charter, art. 2(4)) and to "settle their international disputes by peaceful means" (UN Charter, art. 2(3)). The law of the sea, the law of treaties, the law of state responsibility, international human rights law, the law of armed conflict and every other branch of international law apply in the Arctic as in other regions of the world. Are there points of convergence between Arctic law and international law applicable to AI/ML in the WWC value cycle?

While the principal international law conventions do not explicitly address AI/ML in any domain, certain uses could implicate and possibly breach international law. For example, an AI-driven cyberattack could run foul of the UN Charter requirement to maintain international peace and security and promote friendly relations among nations, and fundamentally the principle of sovereign equality that is the cornerstone of the international system. In a conflict context, the use of AI/ML algorithms could violate the fundamental principles of proportionality and the required distinction among combatants and non-combatants that underpin the Geneva Conventions and its Optional Protocols. The use of AI for surveillance and data collection might breach the International Covenant on Civil and Political Rights and the International Covenant on Economic, Cultural and Social Rights. And assuming the foregoing uses could be attributed to a state, the international law of state responsibility via commission or omission might be implicated. All of these have the potential to implicate the data streams, forecast systems and services provision of the WWC value cycle.

There is generally applicable law, including soft law, but no international law specific to the subject, i.e. a *lex specialis*. However, a constitutive process – i.e. the law-making that could implement the authoritative decision structures of the algorithmic north – is evolving. A number of international legal instruments and state practices that generate customary law apply to AI/ML for Arctic weather. UNCLOS and the Chicago Convention regulate many of the platforms on which sensors are deployed. Satellites operate under the Outer Space Treaty and associated licensing regimes. Coastal and flag states cite UNCLOS (parts II and V) and the Chicago Convention to regulate sensors in their territory, exclusive

economic zones and airspaces, while indigenous peoples invoke CARE-based data sovereignty for observations drawn from traditional lands. Against this backdrop, the WMO's non-binding instruments – Resolution 40 (meteorology), Resolution 25 (hydrology) and the 2021 Unified Data Policy – urge its 193 member states and territories to share "essential" observations freely and in near-real time. Each of these domains channel authority, yet none was designed for algorithmically mediated forecasting in the Arctic.

International and regional organisations are at the centre of this constitutive process, and paramount is the European Union (EU), whose regulations apply to much of the Arctic. The EU General Data Protection Regulation that entered into force in 2018 is perhaps the most effective international data protection privacy law, which though a regional instrument has global reach. The EU has produced useful Ethics Guidelines for Trustworthy Artificial Intelligence in 2019, but being guidelines, they are voluntary. In 2021, the United Nations Educational, Scientific and Cultural Organization (UNESCO) adopted Recommendation on the Ethics of Artificial Intelligence with the aspiration that it would establish a universal normative framework for member states.[9] The UN General Assembly established a multidisciplinary Independent International Scientific Panel on Artificial Intelligence in August 2025 and launched a Global Dialogue on AI Governance on 25 September 2025. Among the themes that have emerged is the use of AI in autonomous weapons systems, which the International Committee of the Red Cross (and humanitarian non-governmental organisations are seeking to ban. But weather has not been mentioned in this context apart from its implications for climate governance.

Like the runner in a pack attempting to catch up with the lead, the constitutive process is racing to catch up with the technology – And effective regulation is by no means assured. States may sequester weather and water observations behind paywalls or security filters. Once Arctic measurements cross borders via cloud infrastructure, they encounter external frameworks such as the EU's General Data Protection Regulation (2016/679) and Asia-Pacific "data-free-flow" accords, triggering adequacy reviews and localisation debates – even when the issue is ice thickness rather than personal information. Maintaining access, ensuring quality, and respecting state control therefore demand interoperable metadata, reciprocity clauses, and codified accountability chains from sensor maintenance to algorithmic output. Absent such safeguards, geopolitical contestation and cyber interference have the potential to sever the chain on which these systems rely.

There are two key law-making challenges: prescription and application. The prescriptive imperatives are universality, specificity and complementarity. High North weather, water and climate services are part of a global system, and thus subject to universal legal instruments. However relevant international law must include the specificity to address and regulate regional realities, while the mosaic of emerging prescriptions must be complementary, cross-referencing

[9] The United States will withdraw from UNESCO effective 31 December 2026.

AI/ML uses and platforms. The other law-making challenge is application, i.e. ensuring that authoritative decisions are controlling and hence truly law. This requires the commitment of states and powerful corporate actors, including, plausibly, AI systems themselves. Heretofore, principle High North state actors have been Arctic Council (AC) states and non-AC polar-capable states such as China and India. However, the war in Ukraine, the advent of more non-AC polar-capable states, the reduced US government commitment to Arctic science, and now the widespread adoption of AI/ML technologies are eroding the AC model of Arctic governance. The key driver is AI – as power.

Innovation, risk and the common interest

In the High North, accurate forecasts and timely warnings are indispensable for safeguarding human life, enabling secure military and civilian operations, supporting fisheries and industry, and ensuring the resilience of critical infrastructure in an environment where small errors can have outsized consequences. The risks are both real and elevated.

The rapid entry of cloud and AI megavendors into the polar weather, water, and climate enterprise turns them into de facto critical infrastructure – yet they answer primarily to shareholders (and somewhat to customers), not to safety standards, domestic authorities or international conventions. Platform contracts can bundle-compute credits, proprietary neural weights, and long-term data hosting in ways that lock national meteorological and hydrological services into opaque ecosystems, undermining the WMO principle of free and unrestricted exchange and having the potential to slow down in-house development. Because these firms sit outside the web of international agreements that bind public providers, export-control clauses or commercial disputes can abruptly throttle access to training data or ensemble output, with direct repercussions for member states. Early adopters in insurance, shipping and resource extraction already shape model design through bespoke risk metrics, skewing optimisation toward insured assets rather than unmonetised community impacts. Absent hard regulatory guard rails – competition-law remedies against vendor lock-in, compulsory licence escrow of critical weights, and public-interest overrides on service continuity – the Arctic WWC value cycle risks becoming dependent on proprietary black boxes whose failure modes and withdrawal thresholds are set by quarterly earnings, not by polar safety standards.

Furthermore, AI-enabled weather, water and climate services in the Arctic now sit squarely inside the threat envelope of hybrid conflict. Adversaries no longer need icebreakers to wreak havoc – a cleverly aimed cyber packet or radio pulse can do the job. UN telecom, aviation, and maritime agencies warned in March 2025 of a surge in GNSS jamming and spoofing that could blind autonomous vessels and sensor buoys, severing the positional “truth” on which predictive models depend. Meanwhile, the AI/ML stack is itself an

attack-surface[10]: data- and model-poisoning can seed forecasting engines with imperceptible errors or sleeper backdoors, degrading safety-critical outputs at scale. Arctic operators must therefore treat WWC data flows as critical infrastructure. This will require concerted efforts to harden downlink stations, implement satellite-independent timing fallbacks, audit training corpuses and embed zero-trust provenance checks from sensor to inference. Integrating cyber-physical resilience into existing Polar Code duties and bilateral search-and-rescue compacts is no longer optional; it is the *sine qua non* of situational awareness in the algorithmic North.

In the context of the unprecedentedly rapid evolution in AI-/ML-based approaches, shared-liability architectures are emerging, but in a sometimes reactive or haphazard way. The WWC value cycle in the Arctic is already a house of cards, comprising enforcement-free standards and regulations, diverse bilateral agreements, divergent paths to legal redress, and regional light governance agreements overlain by sector-specific sources of international law. It only works through goodwill and self-interest, supported by largely inadequate aid efforts like the WMO Systematic Observations Financing Facility. The rapid introduction of AI/ML approaches is a chaotic force, throwing the sector perhaps catastrophically out of balance. The algorithmic North is rapidly building dependencies on systems in an institutional vacuum. The potential for a range of undesirable futures from anarchy to algocracy is evident. The AI/ML power shift must be addressed – and rapidly – with proactive policies that balance the critical enablers of open innovation, secure authority, and controlling regulation in the interests of states and their people. Effective policies can become prescriptions and, when backed by state power, become applicable law.

To navigate this algorithmic transition without undermining the Arctic WWC system, policy action is across three domains is imperative. Firstly, international organisations, led by the WMO as the responsible agency, must clarify the value proposition of public-private partnerships. Public data, when open-source and standards-driven, provides the provenance and traceability needed to train robust models and defend against adversarial attacks. It is critical that this be enshrined in clear exchange for access to publicly supported, high-quality, technically compliant data. Secondly, international law as an instrument of policy must be galvanized. The problem is not the paucity of prescriptions, but the uncertainty and inadequacy of their application. Existing regulations and soft law can only be made effective as binding international law when the political will of states is motivated in the domain of algorithmic forecasting. This is a legal problem *and* a policy problem. Thirdly, with respect to security policy, the expanded threat surface[11] posed by hybrid AI/ML infrastructures

[10] An attack surface is the sum total of all possible entry points and vulnerabilities that an attacker can use to compromise a system, network or organisation.

[11] A threat surface is the sum of all possible vulnerabilities and attack vectors in a system or network that an attacker could exploit to gain unauthorised access, steal data or cause damage.

demands urgent attention. While no system can be made invulnerable, shoring up the first two domains creates conditions for resilience under duress. Hence a priority for national security decision-makers is to ensure that data in the WWC system is tagged to protect against the poisoning of model-training corpuses, both public and private.

Ultimately, it is not enough to react to each emergent challenge of the algorithmic North in isolation. The essential and most vexing global policy task will be to clarify the common interest.

Annex

Table 1: Taxonomy of methods for WWC services from classical optimisation to current AI/ML approaches

The seven task categories in Table 1 trace a continuum that begins with long-standing assimilation techniques such as four-dimensional variational assimilation, passes through hybrid physical-statistical emulators, and culminates in fully data-driven generative and decision-support systems. Presented side by side, the categories clarify how each method underpins a distinct operational function within the WWC value cycle.

Task category	Core purpose	Illustrative Arctic-use case	Indicative techniques
Data-sparse gap filling	Reconstruct missing, biased or poor-quality observations	Inferring sea-ice cover when seascapes are obscured by clouds	Gaussian process regression; variational auto encoder; random-forest imputation
Multimodal data assimilation	Integrating heterogeneous data streams to initialise numerical weather-prediction models	Blending satellite-derived profiles with ship and buoy data for storm forecasts	Ensemble Kalman filter; four dimensional variational assimilation; transformer-based sensor-fusion networks
Hybrid physical-statistical emulation	Accelerate or replace sub-grid scale or full dynamical cores	ECMWF AIFS global surrogate and Bris stretched-grid GNN model capturing polar lows over the Nordic seas	Graph neural networks; attention-based transformers; diffusion probabilistic models; continuous ranked probability score-optimised ensembles
Probabilistic post-processing	Calibrate raw model output into impact metrics	Translating ensemble wind fields into ice-ridge exceedance risk for vessels	Ensemble model output statistics; Bayesian model averaging; quantile regression forests
Event discovery and classification	Detect and label extremes in near-real time	Flagging polar lows and heat-wave pulses from satellite feeds	Convolutional neural networks; vision transformers; object-detection frameworks
Scenario downscaling	Produce high-resolution climate projections	Generating 2 km coastal flood maps for Nuuk under a climate-change future scenario	Generative adversarial networks; diffusion probabilistic models; super-resolution convolutional neural networks
Decision-support orchestration	Couple forecasts with socio-economic data	Optimising asset pre-positioning along the northern sea route	Reinforcement learning; Bayesian decision networks; multi-agent reinforcement learning

Building Peace Together

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-440-0

GCSP
Geneva Centre for Security Policy