THE NEXTGEN INFORMATION ENVIRONMENT

THE NEXTGEN INFORMATION ENVIRONMENT

ISBN: 978-9934-619-76-2

Authors: Neville Bolt, Elina Lange-Ionatamishvili
Design: Tornike Lordkipanidze

Riga, February 2026

NATO STRATCOM COE
11b Kalnciema iela
Riga, LV1048, Latvia
stratcomcoe.org
@stratcomcoe

CONTENTS

BACKGROUND TO THE REPORT

AIM OF THE PROJECT

NATO Strategic Communications Centre of Excellence (NATO StratCom COE), based in Riga, Latvia announced its **NextGen Information Environment** project in early 2025. It convened renowned international experts from academia, policy-making, and business to answer a number of questions:

How will immersive and emerging technologies redefine public interaction with information? Furthermore, what forthcoming technological advances should we anticipate, and what early indicators should we track to gain a nuanced understanding of how these innovations will reshape geopolitical power dynamics and influence the resilience of democratic processes?

IMPLEMENTATION AND ACKNOWLEDGEMENTS

The NATO StratCom COE held a number of interdisciplinary research meetings in 2025. These took place at the University of Cambridge (3-4 March), in Riga (12 June), at the University of Oxford (15-16 September), in Riga (11 December). The sessions were convened in association with Sympodium Institute for Strategic Communications, London.

Fields of expertise represented included Artificial Intelligence; Cyber security policy; AI Ethics; Defence economics and innovation; Economics and digital society; Futurism; Global history; Geopolitics, technology, and global markets; History of Technology; International security; International law; Interdisciplinary Ethics; Moral, political, and legal philosophy; National Security; Political science; Philosophy of Artificial Intelligence; Social psychology; Sociology; Strategic Communications; Technology.

Expert participants who attended some or all meetings, and subsequent conversations were:

Chiyuki Aoi, Renaud Bellais, Roland Benedikter, Neville Bolt, Audrey Borowski, Nick Bostrom, Louis Brooke, Judith Buchanan, Nicholas Butts, Doug Chalmers, Yaqub Chaudhary, Andrew Cheatham, Diane Coyle, Benjamin Delhomme, David Deutsch, Lloyd Dorfman, Linda Eggert, Jakob Foerster, Peter Frankopan, Markus Gabriel, Marija Golubeva, Vitaliy Goncharuk, Lucas Greenbaum, Andrew Hoskins, Felix Karte, Philipp Koralus, Yara Krushchenko, Elīna Lange-Ionatamišvili, Benjamin Läpple, Richard Ned Lebow, Doowan Lee, George Lee, Eglis Levits, Sander van der Linden, Carl Miller, John Naughton, Gina Neff, Jonnie Penn, Anders Sandberg, Jānis Sārts, David Scheffer, Päivi Tampere, Linnar Viik.

NATO StratCom COE wishes to thank all our contributors who gave generously of their valuable time and rich insights. We are grateful to the Masters of Emmanuel College, Cambridge, St Peter's College, Oxford, and Gonville & Caius College, Cambridge for their kind support.

FOREWORD TO THE REPORT

Nations around the world recognise the importance of adopting emerging technologies to benefit their societies. NATO is no exception. Technological advantage is seen as vital on the field of battle too where scientific innovation, industrial application, and economic progress have historically gone hand in hand. Equally important are the consequences of emerging technologies for the way that NATO and its member states project their strategic communications to other nation states, no less their own populations. While allowing governments to understand and engage with their citizens more directly, these new technologies also pose a number of risks which are becoming increasingly apparent. For one, NATO foresees information operations enabled by artificial intelligence (AI) affecting the outcomes of democratic elections; indeed sowing confusion and division across alliance states, while further undermining and fracturing societies and their militaries in times of conflict. And all set against a backdrop of waning trust in national institutions and authorities.

NATO takes a particular approach to the way it understands strategic communications. Rooted in its genesis, the Washington Treaty of 1949, which proclaimed a mission to protect and preserve the fundamental freedoms of its member states and their citizens, it would more recently re-articulate that commitment to its liberal democratic offering. Terminologists and doctrine writers circumscribed the field of strategic communications by refreshing its list of qualifying criteria. Perhaps the most strikingly ambitious of which is its commitment to project visionary consequently long-term positive change, in the human condition. But how should that be achieved when the future appears ever more uncertain and the very technologies societies are embracing have begun to display inherent illiberal, if not authoritarian tendencies?

As a targeted approach to promoting liberal democracy and as a field of political and geopolitical influence, strategic communications is no less ambitious. Today NATO finds itself at an historic moment. A rapidly changing world has witnessed the return of Great Power politics, the dramatic acceleration of digital and emergent technologies, a retreat from liberal globalisation and reassertion of mercantilist trade, accompanied by a number of wars, one of which is being brutally fought on NATO's border inside Ukraine. Together these so-called poly-crises add up to a recipe for turmoil and unpredictability. But one key crisis should not be overlooked: the fracturing of the post-1945 liberal consensus under pressure from forces inside its borders and from those attacking it from without. The liberal tendency is fragmenting into an array of techno-libertarians, nativist libertarians, liberal democrats, and illiberal democrats as a drift to broader authoritarian values, populism, and demagoguery takes hold amid covert and overt onslaughts from states such as China, Russia, Iran, and North Korea.

Such is the context for a number of constraints leaders of the alliance face. As a defensive

political-military alliance NATO's institutional remit falls short of addressing even the majority of these changes in the international landscape. However, one in particular, looms large: what has been described as a new arms race between China and the US concerns artificial intelligence. And it highlights an inherent vulnerability of the alliance whose member states, but with some significant additions, map approximately onto the member states of the European Union. In this complicated geography, geopolitical direction is ultimately set by political leaders of both the alliance's and the union's individual national governments.

Meanwhile technologies come with merits and demerits. AI arrives with the promise of societal transformation. The alarming acceleration of its development, however, has found many governments leaden-footed, and its regulatory and judicial processes unable to keep pace. For many governments in the democratic West, AI continues to be viewed as a sophisticated tool. For others it represents the emergence of a new information and communications eco-system capable of transforming the way human beings connect ontologically to the world outside themselves in the 21st century. The growing fear is that by failing to recognise and project the transformational aspect of these new technologies with their threats and benefits, not only will European democracies fall irretrievably behind in a high-stakes contest involving China and the US, but they will reinforce a natural conservatism and risk-aversion already inherent in pluralist democracies with their short (re-)election cycles. At the same time, the interventionist and regulatory tendencies of democracies that wish to exert greater controls over dynamic capital markets compound a growing trend to short-term thinking. Overall, short-termism in democracies or democratic presentism, comes to privilege the rhetoric of pragmatism over idealism.

Proponents of strategic communications see an opportunity here not only to break out of short-term thinking but to encode an ethical alternative into a set of technologies that display autocratic tendencies so attractive to authoritarians. By promoting a value system, they argue, grounded in a responsible calibration between the symbiotic forces and counter-forces of legitimacy and persuasion, versus authority and use of force, a 'values-first approach' would offer a moral compass currently absent from debates surrounding artificial intelligence. To harness revolutionary technologies to a moral purpose rather than technocratic or operational function only underlines the importance for Western democracies to innovate economically to benefit their future societies in the long-term.

The NextGen Information Environment sessions convened throughout 2025 sought to address these concerns and a number of other recommendations captured in this report.

KEY

OBSERVATIONS

- NATO faces a new kind of Cold War, defined by high-technology competition. Adversaries employ emerging technologies to target citizens of NATO member states.

- The shift in thinking to offensive rather than defensive strategic communications has already occurred. The critical question is what form it should take.

- The security domain is hybridised. Private actors exert growing influence and operate with significant autonomy. Commercial entities and technology leaders directly influence strategy and security, sometimes independent of state control or alignment.

- Policy makers are caught in the dilemma of treating artificial intelligence as an economically progressive tool while failing to recognise fully the technology's ability to transform our lives. This lack of clarity that derives from inadequate literacy in science and technology, particularly in government policy making circles, produces a security concern.

- Europe remains cautious, prioritising regulation, promoting ethics, but limiting practical experimentation. Without hands-on experience, a Europe short on political will, risks falling irreversibly behind its competitors. Europe should balance a desire for greater transparency and trust with more open access to data to enable the private sector to experiment through public-private partnerships.

- Neuro-warfare is emerging, requiring urgent attention. This convergence of human and machine surpasses artificial intelligence to become a neurotechnological revolution with profound implications for democracy and the information environment. Predicting human consciousness and interpreting neural data are not theoretical, they already exist.

- In future, information warfare will depend on mathematical calculations made by machines to determine message advantage. Agentic systems will constantly evaluate and attempt to out-compete each other.

- A new front in information warfare entails the deliberate poisoning of Western open-source AI models by injecting false data designed to corrupt future training cycles.

- Institutional trust will decline as information environments become more personalised and decentralised through micro-targeting. Users will come to expect autonomy and customisation, but distrust authority, expertise, and institutional mediation.

- Knowledge is a strategic currency. Influence over what counts as knowledge, how it is summarised, and who owns it is now being contested. Where authorship and authenticity are in doubt, AI systems could become the most trusted actors. Conversely, parts of society might lose trust in AI systems due to their perception and fear of data poisoning and manipulation.

- Advanced AI systems may fragment evidence with competing interpretations of objectivity that use different algorithmic frameworks. They shift the burden of proof from evidencing allegations according to agreed and entrenched standards to choosing which AI-mediated system has the authority to define what constitutes valid evidence.

- AI's 'licence' to make independent decisions depends on safeguarding transparency, public audit, and democratic oversight. Absenting humans from decision making risks reinforcing autocratic tendencies in technologies.

EXECUTIVE

SUMMARY

A

dramatic transformation driven by emergent, digital technologies is taking place in the early 21st century. Machines no longer simply enable human communications: they communicate independently drawing on their own decision-making ability. And they are functioning in an information environment increasingly understood as an ecosystem of contested ideas and influences.

Society is transitioning into a new historical era where seeing no longer constitutes believing. Truth and evidence fall victim to new technologies able to blur the lines between fact and fiction. Significantly, they support the ambitions of malign actors both within and beyond sovereign borders who would take advantage of this ambiguity to subvert pluralist and majoritarian democracies.

What are these new technologies, what future do they promise, and how will they shape the way humans see the world? While the US and China have prioritised developing these innovations, a hesitant Europe appears caught between a number of competing tensions. Should it challenge this binary competition with a home-grown artificial intelligence stack or instead regulate in the hope of preserving its liberal democratic traditions? Or is a piece-meal approach the likeliest outcome? Europe's technological future will impact NATO's capabilities and global positioning.

THE FUTURE INFORMATION ENVIRONMENT

Some plausible scenarios for the future of the information environment are outlined below. They recognise the inherent difficulty of predicting outcomes shaped by interdependent factors – political transformations, technological discoveries, ecological crises, even natural disasters – that may shift centres of power, consequently affecting the ways technologies develop in unforeseen ways. There can be no claim to certainty. Nevertheless, we identify critical vulnerabilities and vectors of attack drawing on expert discussions conducted throughout this project. Informed views guide our focus on certain threats for which NATO and its allied countries should make far-reaching preparations over the next decade, regardless of which of these future scenarios materialises.

Complex Security Landscapes

The future will see competition for technological infrastructure that offers access to populations in an attempt to influence the way people think and speak.

Non-democratic actors may increasingly offer open-source solutions to assert their positions in a marketplace of emerging technologies. That could create strategic vulnerabilities on two fronts. By adopting apparently 'neutral' systems into their societies, Western democracies risk embedding ways of thought

imbued with authoritarian values, as well as means of surveillance and algorithmic biases. At the same time, dependencies can be created that will be difficult to reverse once particular infrastructures become dependent on them. Concurrently, it is feasible that authoritarian actors will extend their reach into the Global South by offering subsidised open-source systems, while undercutting Western commercial products. Such a development would allow them to shape different information environments and further influence the broader international digital infrastructure. A normalisation of authoritarian technical logic and its foundational ideologies would ensue.

Private actors – commercial entities and individual technology leaders – may be able to exercise unprecedented influence with direct strategic outcomes while operating independently of state control. Leading technology corporations navigate between states, but supply a variety of states (including some ideologically opposed to the West). The way technology leaders view the world and the nature of their ideological commitment will have strategic consequences. The hybridisation of security and information landscapes, which is already under way, will be exacerbated.

The Fragmentation of Reality

Contemporary social media will probably change. Instead, immersive environments guided by AI avatars are expected to deliver rich, adaptive experiences tailored to individual preferences and emotional states. Personal AI agents will then curate not simply information but experiences, by adjusting content dynamically, offering different styles through which consumers interact, and diverse personal stories through which individuals understand their own identities.

Micro-targeting leads to hyper-personalisation. In turn, parallel but individualised realities rather than shared discourses come to dominate human consciousness. Micro-targeted content may then fragment societies into self-contained and introverted communities where accepted information becomes isolated, and where facts, references, and values have little common ground. Similarly, privacy and access to verified 'quality information' will depend on a consumer's ability to pay, potentially creating further inequality and divergence in perceptions.

Advertisers and those in positions of influence could refine the way they construct accepted accounts by adapting them to populations which have been digitally replicated to mirror targeted demographics. By which time, institutional trust may have declined to such a degree that users continue to assume and demand personal autonomy but place greater trust in AI systems than they do in human authority or expertise. As everyday human and AI-generated communication become increasingly indistinguishable, and audiences grow accustomed to synthetic content, this tendency may elevate AI to become the most trusted authority.

The Algorithmic Battleground

The future information environment will be shaped by autonomous systems operating beyond direct human oversight, leading towards full automation of information operations in parts of the system. Agentic AI systems will constantly interact at scale, filtering, curating, and choosing what kind of information attracts human attention. Machines thus gain a strategic advantage. Adversaries, in turn, could use digital replicas of populations to test whether their algorithmically-optimised content will influence human audiences once filtering and curating systems have been successfully manipulated to connect to them. Influence operations will take the form of algorithmic competition where machines target other machines, and where the best mathematical processes come to dominate, while systems attempt to outperform each other in determining which information campaign wins out.

The Contaminated Information Ecosystem

The trend for Western open-source AI models to be 'poisoned' systematically by injecting false data into training cycles and designed to corrupt them will probably increase and become an essential 'arm' of future information warfare. Adversaries will subsequently reverse-engineer AI, creating content specifically designed for machine consumption rather than human persuasion. Specialised models may prove easier to manipulate. These could include synthetic training data – artificial models designed to corrupt how other models understand reality. A world is born where AI systems trained on synthetic audiences or their digital representations produce distorted outputs.

The Crisis of Knowledge Authority

AI systems could become the most trusted actors in environments where human authorship and authenticity are consistently in doubt. Knowledge authority will then have shifted from democratic institutions to technical systems, creating new dependencies and vulnerabilities susceptible to infiltration by adversaries. Different AI frameworks will produce competing interpretations of objectivity, moving debates from the need to prove assumptions according to agreed standards of argument and evidence gathering, to determining which algorithmic system has the authority to define what evidence is actually valid.

AI will provide not just information but emotional support and companionship. Embedded emotional intelligence will be able to influence making choices, beliefs, and behaviours. Which opens up new vulnerabilities to psychological exploitation and manipulation, particularly among individuals already isolated in their communities or groups, and where people's relationships with AI begin to supplement or replace human interaction.

The Erosion of Shared Foundations

The question then will not be whether shared information environments exist. Rather, whether historic environments can be preserved. Common understandings founded on fact – a prerequisite of democratic discourse – will come under severe strain from commercially curated algorithms. Not to mention adversarial manipulation. And the absence of trusted institutional gatekeepers capable of establishing authoritative truth-claims across fragmented micro-publics will only exacerbate the problem.

This environment will demand not just defensive measures but offensive strategic communications. Democracies will feel the need to engage in 'cognitive warfare', at the same time promoting ethical frameworks that distinguish them from authoritarian approaches.

The Neuro-technological Revolution

Soon, neural data will become a critical asset for commerce and governance. Neuro-technology's power derives from its convergence with AI systems. This fusion will establish neuro-warfare as a major security domain, with AI-enabled neurological modelling. The convergence of human consciousness and machine interpretation will profoundly affect democratic processes and information integrity. Capabilities to predict consciousness and interpret neural data will become a regular part of operations. Neurological modelling – creating representations of how individuals think and feel – will move towards unprecedented precision in psychological manipulation.

POLITICAL ACTION

Based on the project's findings, we have created thematic clusters of key questions to consider and possible action points for Allied governments.

Security Landscape and Information Warfare

Neuro-warfare represents an emerging field requiring urgent attention. NATO allies should place greater emphasis on creating units dedicated to anticipatory analysis. These should focus on the frontiers of neural data, and address current institutional gaps.

A strategic shift is taking place from content creation to influencing curation and filtering. It should be addressed by ensuring the necessary understanding and capabilities, are in place, including detection and countering measures.

Western democracies should change the way they think about security from frameworks where counter-narrative inevitably responds to narrative, and instead identify how best to impose costs on adversaries by conducting technology-enabled information operations.

Western governments should acknowledge the increased influence of private sector technology leaders and anticipate how to address the implications that arise from misalignment between private and state interests.

The proliferation of agentic systems invites urgent attention. As automated agents increasingly interact at scale beyond human oversight, they filter and negotiate the relevance of information in ways that are vulnerable to manipulation.

Western states should develop systems to detect and mitigate threatening content designed for AI consumption, and map emerging domains of influence operations that adversaries target.

Democracies should safeguard against adversaries who seek to acquire or infiltrate companies that manipulate search engines and reverse-engineer or poison large language models. National security frameworks should assess acquisitions of digital platforms driven by political objectives and information control rather than commercial logic; thus intervene where strategic threats emerge subject to respecting legitimate market freedoms.

New governance frameworks are required to address the shift from trust in institutions to AI. AI systems with embedded emotional intelligence create new vulnerabilities to psychological exploitation, particularly where adversaries can infiltrate systems capable of shaping human judgement.

Growing competition with China requires Western policy makers and public actors increase their Sino-literacy to address a dangerous asymmetry in information.

The liberal democratic West should explain why moral supervision is required over surveillance technologies that function indirectly. Foundational ethical frameworks should be put in place to address social problems that arise from technologies' tempting appeal before they are adopted.

AI systems in authoritarian countries are only partially under the control of political authorities. This opens up strategic vulnerabilities, creating fresh opportunities for liberal democracies. Populations in authoritarian countries could still access AI systems that generate common knowledge which may yet fall outside regime control and offer the opportunity to undermine authoritarian stability from within.

NATO's defence spending commitment of attaining 5 per cent of GDP invites clarification. In particular, how resilience should be newly defined to address new challenges, and how funds should be allocated to build resilience in information environments.

NATO's offensive strategic communications capabilities require a greater presence in virtual information environments. That involves pre-emptively engaging in contexts of 'cognitive warfare' with moral frameworks that justify offensive operations in the face of adversaries who use technology to undermine democratic stability.

Europe should strengthen its de-platforming and de-funding strategies by employing frameworks like D-RAIL (Directing Responses Against Illicit Influence Operations). At the same time, it will be necessary to prepare for an inevitable policy confrontation with the US over divergent standards of de-platforming.

Political Vision

Strong political vision and effective leadership are required if short-termism is not to be further institutionalised.

The European liberal democratic project needs to be re-energised if it is to restore internal legitimacy and global competitiveness. A renewed sense of mission, backed by substantial capital investment, would provide the foundation for revival.

More agile, risk seeking, and decentralised forms of democratic organisation are necessary, driven by strategic priorities that are clearly communicated. Balancing ambition with tangible results is key.

A credible governance model should prioritise a focused set of long-term objectives. This requires aligning public, private, and academic sectors to pool resources across nations while rewarding excellence, eliminating duplication, and deploying assets more efficiently.

Democratic principles should be embedded in AI governance from the outset. It is naive to assume that deregulation and economic growth alone will protect liberal values. Early choices will determine whether AI enables freedom and innovation or facilitates authoritarian control.

Regulatory authority should be strengthened to counterbalance corporate power that currently exceeds state influence in key technology sectors. For Europe, this represents a sensitive balance between building on but extending the Digital Services Act framework, and loosening excessive regulation and bureaucratic processes.

If Western democracies genuinely aspire to protect liberal values and improve the quality of human life, it is incumbent on them to refresh the ways they try to understand humanity, and its ambitions and needs, by harnessing contemporary conceptual frameworks that look to the future.

Normative Foundations

Defending democracy demands a novel infrastructure of anticipatory governance. New forms of interdisciplinary teams who can integrate research, business, and politics will be needed to determine which futures are desirable for humans before translating those insights into more realistic policies and regulation.

The liberal democratic West is built on a rich foundation of normative values. It should cultivate a diversity of models, anchored in equity, transparency, accountability, and its particular value system, committed to human rights and dignity.

Liberal democracy's future may depend on establishing 'ethical environments' that integrate ethics into technology, capitalism, and social systems. Addressing defence and security challenges becomes a prerequisite to creating stable spaces where ethical frameworks can take root.

Technical solutions alone cannot resolve questions of values and purpose. Governments should distinguish technical problems from normative questions requiring democratic deliberation rather than data-driven solutions.

Protecting democratic knowledge requires safeguarding epistemic diversity. AI systems should be designed to preserve multiple ways of gaining knowledge, including the ability to draw on epistemologies of indigenous minorities and their interpretative traditions, rather than directing hegemonic knowledge to algorithmic outputs.

Liberal democracies should reject the assumption that the current digital infrastructure is inevitable. Proactive governance can shape architectures to prioritise privacy, security, and democratic values through open-source alternatives and pre-emptive regulation which applies to specific products.

Restoring trust in institutions demands transparency about how decisions are made. Public authorities should move away from 'black box' decision-making by explaining which forms of evidence were considered, how competing perspectives were weighed, and why particular conclusions were reached in any decision making process.

Liberal democracy should confront fundamental questions about human progress. Defining acceptable boundaries to technological development – particularly in military contexts – may require creating new humanist frameworks that renew core assumptions of what it means to speak of human dignity.

Education represents a critical frontier where AI's influence over how humans learn constitutes a profound shift in the ways ideas and values are transmitted at scale, requiring democratic oversight.

Transparency and Accountability

The liberal West should advocate for true openness in AI – transparency about design principles, training data and parameters, system prompts, and model weights – so that the origins and biases of models can be understood and publicly debated. Emphasis should be placed on AI model training that can be fully reproduced. Clear distinction between raw data, interpreted evidence, and human judgment are required in automated processes.

Democracies would benefit from promoting open-source, decentralised AI alternatives that prioritise user agency, open standards, and audit over proprietary systems that are developed beyond democratic control.

Reducing algorithmic bias requires understanding context. Investing in training AI systems with an awareness of cultural, historical, and social context enhances transparency and helps prevent the perpetuation of discriminatory patterns.

Allied nations need technical regulatory authorities to audit and validate AI systems that turn principles of governance into operational oversight. Strong institutions should ensure responsible deployment and provide effective remedies when technology causes harm. Effective frameworks for accountability, liability, and due diligence are needed to address the growing autonomy of coding agents and other agentic systems.

Maintaining common values built on shared foundations based in facts requires deliberate institutional design, not market-laissez faire. Democracies should invest in algorithms that serve the public interest, transparent systems to make recommendations, and mechanisms for verification that detect synthetic content while preserving shared factual foundations.

Hyper-personalised information environments risk fragmenting societies into communities of incompatible realities. ‘Cognitive warfare’ requires a coordinated Western response. Safeguards against micro-targeting, information and algorithmic manipulation should be put in place to protect individuals from efforts to erode public confidence and polarise societies. Similarly, robust frameworks of accountability are needed to trace the responsibility for controlling personalised information to specific actors – whether commercial platforms, state agencies, or foreign adversaries.

Surveillance capitalism is not a technical necessity but a political choice which can be challenged by regulating the monetising of data, mandating processes of decentralisation, and developing open-source alternatives. Democracies can reject the ways industry frames and conflates the extraction of behavioural data with protections of individual privacy, recognising that systems are politically constructed and reversible in the democratic interest rather than technically inevitable.

Decentralisation and Market Incentives

Pluralism, diversity, and healthy competition remain central to resilience. Translated into technologies, it means multiple actors and approaches rather than development of a single, centralised model.

Adapting regulatory and market conditions to encourage ‘fast moving tech cells’ in parts of Europe would speed up innovation and Europe’s global competitiveness.

New market incentives should be introduced to create ethical technologies that safeguard the public interest. Those may include tax benefits, procurement preferences, and regulatory advantages.

Public-private financing and research investment remain inadequate. A revised public investment strategy is essential – one that delivers substantially increased funding quickly, creates opportunities for public-private partnerships, and adopts a more agile approach to taxation and regulation.

Countries can maintain political sovereignty over AI technologies by deploying mixed infrastructure models that keep sensitive data inside national jurisdictions, enable compliance with local legislation, and reduce dependency on foreign infrastructures.

Democratic participation can be protected from AI manipulation through robust authentication and supervised platforms. Decentralised governance systems which rebuild legitimacy without creating new vulnerabilities can be deployed while addressing key challenges: establishing independent oversight to protect fairness, preventing new concentrations of power, and ensuring that technology strengthens collective action.

Current AI systems over-represent dominant cultures at the expense of marginalised perspectives. Europe in particular should address ‘data nepotism’ and require more representative and diverse training datasets to elevate minority perspectives and languages rather than reinforce the overrepresentation of dominant cultures.

Populations who lack adequate digital literacy face risks from the unintentional accumulation of data. Individuals may inadvertently create extensive digital footprints that live indefinitely. This in turn enables retrospective surveillance – allowing past behaviour and associations to be scrutinised, often out of context or according to different standards or norms – which can lead to lasting reputational harm. Preventive protections are required.

Gaming environments may offer untapped potential for democratic engagement. Developing distributed platforms run by communities that collaborate to resolve real-world problems could strengthen ethical strategic communications and broaden participation in addressing shared challenges.

Autonomous Systems and Decision-making

AI should be deployed to enhance not displace democratic deliberation.

Liberal democracies should prioritise public trust and democratic legitimacy over operational speed, preventing technocratic governance that erodes shared accountability.

For automated decision-making systems to be compatible with principles of liberal democratic governance, three criteria should be established: mandatory third-party audits and certification; explicable outputs subject to external scrutiny; and processes of democratic oversight. Removing human involvement from decision-making loops may be permissible only once legitimacy has been secured through transparent rules, political accountability, and informed public consent rather than technical capability alone.

Autonomous systems, including in weaponry, require firm grounding in international humanitarian law and human rights. Expertise accumulated in private companies and civic initiatives could be harnessed to develop clear frameworks for rules of engagement, accountability, and verification.

Autonomous drone warfare requires pre-established international frameworks to prevent escalation or operational paralysis during critical incidents. Cross-border contingency plans must address scenarios where drones malfunction, are compromised, or violate sovereignty. Rapid-response legal mechanisms should enable immediate, coordinated action without prolonged diplomatic negotiations, clearly defining liability, intervention authority, and rules of engagement before crises emerge.

Human authority must be preserved in high-stakes decisions involving life, liberty, and public safety. While AI can analyse probabilities and patterns, only human decision-makers can weigh evidence against social values and determine acceptable levels of risk in ways that confer democratic legitimacy. Delegation to algorithms in contexts affecting fundamental rights risks undermining accountability and amplifying embedded biases, regardless of the apparent advantages of performance.

Europe's Economic Competitiveness

Europe should focus on strengthening its position in various layers of the global AI stack while devising a clear investment strategy for critical materials, metals, and technologies, and reinforcing supply chains with more reliable partners.

Achieving digital autonomy could advance Europe's strategic autonomy both symbolically and practically. Public policy favouring European technology investment and procurement could reduce dependency on foreign systems while growing a domestic AI-ecosystem more quickly. Strategic state participation, especially at an early stage, but also sustained industrial financing, may be necessary to overcome systemic inertia.

Europe should rapidly expand its capacity for affordable, reliable energy to retain AI computational workloads that would otherwise migrate to lower-cost jurisdictions.

Europe needs more agile regulatory frameworks that can evolve alongside technological innovation and market dynamics rather than stifle them.

Stringent information and privacy laws and diverse legal regimes between member states make Europe's investment market less attractive and hamper innovation. Harmonisation across member states is essential.

Europe needs accessible data frameworks that enable AI innovation. Private sector access to public and shared datasets requires reformed mechanisms. But protecting individuals' privacy must avoid adding burdensome barriers to users and researchers. Rather than rigid regulation, Europe should embrace flexible approaches to balance individual rights with the data access essential for the competitive development of AI.

Europe should better engage with developing parts of the world by offering its own AI models adapted to local cultural contexts. If Western models fail to serve non-Western users effectively, other actors will fill the gap and export not only technologies but also their ideologies embedded in AI systems.

Innovators express concerns about post-conflict markets from the perspective of viability and sustaining long-term demand. Key questions involve transitioning capabilities into sustainable export markets as wartime demand declines. Concerns extend to include pathways to emerging markets like Africa.

Anticipation and Modelling

AI can be deployed to assist in modelling scenarios for policymakers, while preserving final authority with democratically accountable representatives.

Decision-makers should strengthen their technological capabilities and employ data-driven modelling. AI's capacity can be harnessed to capture societal preferences at scale through tools that aggregate more nuanced understandings of millions of people and forecast long-term societal impacts.

Western anticipation and scenario-based modelling capabilities are lagging. Planning should address catastrophic scenarios, not just incremental disruptions. Critical areas include but are not limited to:

- disruption of AI-driven trading and logistics;
- breakdown of global governance structures undermining the networks technology depends on;
- adversaries replicating key technologies to erode Western AI advantages;
- deliberate poisoning of open-source models through data corruption;
- conflicts involving autonomous systems deployed by actors who disregard ethical constraints and international law;
- preservation of humanitarian protections in autonomous urban warfare;
- compromising of satellite-based computing and data-processing capacity in orbit.

METHODOLOGY

The research sessions spread over a number of days and adopted an impromptu, conversational format. No papers were prepared or presented. A free exchange of ideas was considered to be the most productive means of inviting innovative as well as evidenced thinking about the future. No undue time constraints were placed on individual contributions. No comments have been attributed to any named individual. The first meeting in Cambridge acted as a scoping session to explore and identify which themes and topics appeared most frequently in participants' concerns, and which should be prioritised in subsequent meetings.

The conversations began by employing the following perspectives:

- Developing technological landscapes.
- Acceleration, change, and relationships with technology.
- Authenticity and the relationship with reality.
- Freedoms.

The following themes guided our subsequent inquiries:

- Re-imagining evidence in the future Information Environment (June).
- Sovereignty or autonomy of the AI stack (September).
- Time Horizons, Anticipation, and the Failure to Imagine the Future (December).

This report captures a set of problematics and summarises the primary themes and topics covered during the four sessions. Full summaries of the 2025 sessions will be published by the NATO StratCom COE in spring 2026.

CLOSING REFLECTIONS

An explicit thread connects three key dimensions under review in these pages.

First is the AI stack, the technological infrastructure through which future communications will be disseminated. Who will eventually own it, or more accurately possess their individual stack, will determine how influence is exerted over communications content and processes. If Europe is to be a major actor, then how autonomous or sovereign will be its ownership? Europe's hesitation in investing in independent capacity becomes a question of strategic security not simply geoeconomics.

Second, how will the unique character of this future technology shape – or potentially distort – the evidence-based truth-telling on which European NATO democracies depend? If an ideology of democratic thought can be designed from the outset into a technology which is inherently autocratic, then this becomes a priority for Europe which sees itself as a bastion of liberal democracy.

And third, should this not come about, and all the while emergent and digital technologies develop at a speed few states can understand not to mention control, open information environments will grow increasingly vulnerable to manipulation. Consequently, machines that think for themselves, taking decisions independent of human involvement, present an unprecedented threat to society. The implications for future warfare are clear.

Our focus on Europe reflects the view that European NATO members are falling behind in the global technology race, undermining their ability to shape and protect information environments upon which their future security depends.


EXCELLENCE
solutions
plan
networks
virtual
alliance
expertise
goals
communication
politics
LATVIA
RIGA
evolution
future
respect
concept
NATO
STRATCOM
mission
alternative
strategies
diplomacy
CENTRE
Culture