EUROPEAN LEADERSHIP NETWORK

Federal Foreign Office

Technological complexity and risk reduction:

Using digital twins to navigate uncertainty in nuclear weapons decision-making and EDT landscapes

Policy brief

Ganna Pogrebna
Rishi Paul
Nathan Damaj
Jake McNaughton
Graham Stacey
Immaculate-Motsi Omoijiade

April 2025

The European Leadership Network (ELN) is an independent, non-partisan, pan-European network of over 450 past, present and future European leaders working to provide practical real-world solutions to political and security challenges.

About the 'Simulating Technological Complexity & Advancing Risk Reduction' project

This project focuses on a fast-changing, yet neglected, area of nuclear risk: mitigating the impacts of emerging and disruptive technologies (EDTs) on nuclear weapons decision-making and nuclear command, control, and communications (NC3).

The fundamental aim of this project is risk reduction. We aim to do this by assisting states in identifying and mitigating nuclear-use pathways and potential mistakes / miscalculations generated by the aggregate effects of EDTs on nuclear weapons decision-making processes and NC3 systems.

The 'Simulating Technological Complexity & Advancing Risk Reduction' project consists of three strands of work that seek to better understand EDTs and technological complexity, to produce detailed recommendations to mitigate nuclear risks:

1. **Strand 1** centres on developing a Guardrails and Self-Assessment (GSA) Framework to address anticipated challenges that EDTs pose to NC3 systems and nuclear decision-making.[1] Focusing on technologies likely to mature over the next five to ten years, the framework offers a predictive snapshot grounded in informed assumptions about how these systems may interact and collectively shape the nuclear landscape.

   The GSA Framework examines the combined impact of six key EDTs — artificial intelligence, autonomous systems and drones, counter-space capabilities, deepfakes, cyber operations, and quantum technologies — assessing their cumulative effects and the added complexity they bring to nuclear decision-making processes.

2. Through **Strand 2**, the ELN seeks to create a prototype digital tool that will simulate the highest-level nuclear weapons decision-making instances, the aggregate impact of EDTs in these processes, and the way the framework developed in Strand 1 can mitigate the risks generated by the aggregate effects of EDTs. This policy brief is part of Strand 2.

3. **Strand 3** will develop a sustained campaign to implement the recommendations on EDTs and technological complexity risk reduction among nuclear-weapon and non-nuclear-weapon states and throughout multilateral and supra-national groups, such as the Nuclear Non-Proliferation Treaty review cycle, the Creating the Environment for Nuclear Disarmament initiative, the Stockholm Initiative, and NATO, among others.

This work was performed with the generous support of the German Federal Foreign Office. The views and opinions of authors expressed herein do not necessarily state or reflect those of the German Federal Government.

About the Authors

Professor Ganna Pogrebna
Professor, Executive Director, AI and Cyber Futures Institute

Prof Ganna Pogrebna is an internationally recognised expert in behavioural data science, AI governance, and emerging technology risk assessment. She has previously worked with rapporteurs on AI risks at the Council of Europe, contributed to The Oxford Handbook of Ethics of AI, and published over 114 science contributions. Ganna has led research projects with total funding exceeding AUD 30 million, including projects for the World Bank, MoD (UK), GCHQ (UK), and the Australian Office of National Intelligence (ONI). She is a Methods Editor for Leadership Quarterly and serves on the editorial boards of Scientific Reports and Judgment and Decision Making. Her research focuses on decision-making under uncertainty, particularly in high-stakes environments such as defence, cybersecurity, and nuclear policy. She has advised policymakers on the impact of AI and emerging technologies in national security and crisis management, shaping strategies for risk mitigation and resilience.

Jake McNaughton
Research Data Engineer, AI and Cyber Futures Institute

Jake McNaughton specialises in mathematics, physics, and machine learning applications in high-risk environments. He holds a Bachelor of Science in Mathematics and Physics from the University of Canterbury, an Honours degree in Mathematics, and a Master of Engineering in Bioengineering from the Auckland Bioengineering Institute. Jake's research focuses on the intersection of AI, synthetic data generation, and decision-support systems. Jake is applying advanced computational techniques to nuclear decision-making, using digital twins to simulate complex crisis scenarios and uncertainty models.

Dr Rishi Paul
Senior Policy Fellow, European Leadership Network

Dr Rishi Paul leads the implementation of nuclear policy projects. Rishi's research interests and expertise include nuclear risk and emerging and disruptive technologies, as well as deterrence dynamics in the context of evolving adversarial relationships, especially its effect upon the formation of nuclear strategy and escalation pathways. In late 2022, the Geneva Center for Security Policy (GCSP) awarded Rishi First Prize in its global security competition for "Innovation in International Security". Rishi holds both an MA in Strategic Studies and a PhD in nuclear strategy and ballistic missile defence from the University of Leeds.

Nathan Damaj
Research Data Architect, AI and Cyber Futures Institute

Nathan Damaj has extensive experience in data, systems architecture, and AI applications in finance and security. Before joining AICF, he worked at the Commonwealth Bank of Australia Behavioural Science Centre of Excellence, within its Decision Science and AI division, where he facilitated cutting-edge behavioural research collaborations with leading academics from Harvard, Stanford, Chicago Booth, the University of Sydney, and the University of Melbourne. He was part of the team that developed the award-winning Benefits Finder tool. Nathan has deep expertise in cloud computing, automation, and AI-driven decision systems, with a strong interest in applying emerging technologies to cybersecurity and nuclear decision-making. His current work focuses on leveraging data-driven models to enhance strategic resilience in NC3 systems.

Air Marshal (Ret'd) Sir Graham Stacey KBE CB
Senior Consulting Fellow, European Leadership Network

Sir Graham Stacey is a Senior Consulting Fellow at the European Leadership Network (ELN) and a former Chief of Staff of NATO Transformation, with nearly 40 years of experience in defence and international security strategy. He has served in senior NATO leadership roles, including Deputy Commander of a NATO Joint Force Command, and was Commander and Administrator of the British Sovereign Base Areas in Cyprus. He has operational experience in Bosnia and Herzegovina, the Gulf, Kosovo, Iraq, and Afghanistan, and has served as Senior Advisor to US Central Command (CENTCOM). Sir Graham's work now extends to nuclear risk reduction, with a focus on emerging technologies, military decision-making, and strategic stability in the nuclear domain.

Dr Immaculate-Motsi Omoijiade
Senior Research Fellow and Responsible AI Lead, AI and Cyber Futures Institute

Dr Immaculate Motsi-Omoijiade is an expert in AI, regulatory technology, and emerging technology governance. Before joining the AI and Cyber Futures Institute (AICF), she was an analyst at RAND Europe, a research fellow at the University of Birmingham, and a post-doctoral researcher at its School of Law, focusing on blockchain in healthcare. She is a member of the British Standards Institute's Blockchain Standards Committee and has affiliations with UCL Centre for Blockchain Technology and the Warwick Business School AI Innovation Network. She has advised the UK Cabinet Office and contributed to the African Union's reports on blockchain and AI. At AICF, she focuses on digital twins, AI governance, and nuclear decision-making in complex environments.

Executive summary

This project aims to reduce nuclear risk by helping states in identifying and addressing potential pathways to nuclear use, as well as mitigating mistakes or miscalculations that could arise from the complex interplay between EDTs and nuclear decision-making. As EDTs increasingly intersect with nuclear systems, they introduce new layers of technological complexity that can exacerbate pressures and escalate crises to the nuclear level.

Traditional deterrence models, grounded in static historical data and assumptions, are no longer adequate to navigate this evolving landscape. Digital twins — real-time, continuously updated virtual models of nuclear decision-making environments — offer a dynamic, scenario-based learning tool that enables decision-makers to stress-test NC3 systems, model crisis dynamics, and refine response strategies in real time. By providing structured, evidence-based insights that were previously unavailable, digital twins enhance the capacity of Nuclear Weapon States (NWS) to anticipate and mitigate escalation risks. Originally developed for engineering and manufacturing, digital twins have been adopted in urban planning, aerospace, and military strategy due to their ability to test scenarios, adapt to new data, and enhance strategic foresight.[2]

The ELN and AICF's recent expert testing of a baseline prototype digital twin, between October 2024 and February 2025, replicated aspects of high-level nuclear decision making; it identified that one of their most valuable applications lies in crisis escalation modelling, where they replicate possible nuclear escalation pathways under diverse conditions, including miscalculations, misperceptions, misinterpretations, as well as technical failures and cyber threats. By creating virtual environments that replicate operational complexities of NC3, digital twins can therefore enable opportunities for policymakers, decision-makers, and defence analysts to explore vulnerabilities, assess system integrity, and refine decision-making frameworks to ensure that command structures remain secure and functional under pressure.

This policy brief highlights the critical need for incorporating digital twins as a nuclear risk reduction tool and outlines the potential benefits they offer in strengthening strategic stability. Recognising that states have limited experience in managing security dialogues around the application of digital twins in nuclear decision-making, the policy brief offers preliminary recommendations to address this gap at various levels.

By providing structured, evidence-based insights that were previously unavailable, digital twins enhance the capacity of Nuclear Weapon States (NWS) to anticipate and mitigate escalation risks.

Recommendations

1. **The Stockholm Initiative** has demonstrated a strong interest in addressing the impact of EDTs on nuclear risks and strategic stability, alongside its commitment to advancing nuclear risk reduction measures. It has previously urged the NWS to implement and innovate practical steps to minimise nuclear risks, particularly in pursuit of long-term disarmament goals.[3]

   To advance these objectives, the Stockholm Initiative could create a working group that focuses on identifying and prioritising Guardrail and Self-Assessment (GSA) Framework measures that could be integrated into digital twins developed by NWS and used for EDT - nuclear crisis simulations and NC3 risk assessments, as well as failsafe reviews. While the United States recently undertook such a review under the Biden administration, the other P5 members have yet to follow suit. The Stockholm Initiative could play a constructive role by re-engaging the P5 to include failsafe measures in their discussions, promoting greater transparency in national practices and encouraging the adoption of a best-practice approach to nuclear weapons safety.

2. **The P5** have initiated discussions to enhance transparency around their nuclear doctrines.[4] These efforts should be expanded to include structured exchanges on risk reduction notifications and data sharing, critical components of sustained, long-term risk reduction. As a priority, the NWS should also integrate discussions on the effects of EDTs on nuclear risks into their agenda. Building on this, they should then intensify their commitment to their NPT disarmament obligations, facilitate confidence-building between them, and explore the potential of digital twins as an avenue for exploring the impact of EDTs on nuclear decision-making processes and NC3 systems.

   Although the use of digital twins presents opportunities for nuclear risk reduction, there is a real risk that NWS could misuse the technology to enhance warfighting strategies. Such actions could lower the nuclear threshold and deepen mistrust, with each state suspecting adversaries of using data generated from digital twins as justification for developing pre-emptive strategies. To mitigate the risk of an AI/NC3 race to the bottom and open avenues for shared 'rules of the road', the NWS should commit to sustained dialogue focused on the responsible and transparent use of these technologies. This commitment would lay a foundation for dialogue on the responsible integration of digital twins into their individual nuclear safety and security frameworks.

   A P5 effort to explore these technologies in dialogue could play a pivotal role in fostering trust and mutual understanding, while serving as the starting point for a transparent exchange of relevant risk reduction data. Such dialogue would not only strengthen confidence among the NWS, but also create a shared, evidence-based foundation for informed and responsible nuclear decision-making.

3. **State Parties to the NPT** had agreed in the 2022 draft statement that the NWS should take steps to better understand and mitigate vulnerabilities arising from potentially disruptive technologies and cyber capabilities as they pertain to nuclear weapons.[5] The 2022 Review Conference draft final document reflected an agreement that the NWS would enhance efforts to report on their nuclear arsenals and capabilities, while safeguarding national security, and provide greater transparency on national measures related to nuclear disarmament, including nuclear policies, doctrines, and risk reduction efforts.[6]

   To build on this convergence of positions, NPT State Parties should establish an intersessional working group to examine these issues in depth. The working group should be open-ended to enable representatives from both NWS and Non-Nuclear Weapon States (NNWS) to participate and be co-chaired by one member from each group. Its mandate could be twofold: first, to explore how digital twin technologies can contribute to advancing the Treaty's objectives; and second, to identify practical steps for facilitating technical exchanges between NWS and NNWS on digital twin data related to the effects of technological complexity on nuclear escalation dynamics and risk reduction. It could report to NPT meetings of states parties, leading up to the 12th NPT Review Conference.

4. **NWS** should initiate internal dialogues to assess the feasibility of integrating the proposed Digital Twin Nuclear Decision Framework (DT-NDF) into their national nuclear decision-making processes and identify concrete steps to doing so.[7] Elements of these dialogues should adopt a multi-stakeholder format, ensuring the inclusion of a diverse range of relevant participants, including civil society experts with expertise in digital twin technologies. For the civil society level, a working group could be created to study issues such as transparency in AI-assisted decision-making, preventing misuse of digital twins in the nuclear domain, and ensuring secure and tamper-proof digital twin models.

Introduction

This policy brief examines how digital twins can provide useful data to policy makers to decrease uncertainty under conditions of the rapidly developing EDTs. Unlike traditional simulation tools, which typically do not benefit from having real time data, digital twins are, by design, a virtual environment designed around a two-way flow of information that allow policymakers to engage with structured crises scenarios and explore escalation pathways.[8]

The use of digital twins in assessing vulnerabilities presents risk reducing opportunities for policymakers and officials to consider, such as assessing the effects of technological complexity — the cumulative effects of EDTs — on NC3 systems and refine crisis response strategies under uncertainty. By simulating potential nuclear crises that include the use of EDTs in aggregate, digital twins can provide a data shaping approach to reducing nuclear risks.

Between October 2024 and February 2025, the ELN in collaboration with the AI and Cyber Futures Institute (AICF) conducted structured baseline — low technology readiness level — digital twin testing exercises with a diverse range of transnational nuclear decision-making and EDT experts. These exercises were designed to evaluate how these models, which replicate aspects of high-level decision-making, can identify escalation triggers, assess AI-driven warning systems, and counter cyber-enabled misinformation campaigns.[9]

Although digital twins cannot predict the future, preliminary findings from these exercises indicate that large-scale digital twin models could provide data that enhances decision-makers' ability to reduce nuclear pressures, navigate complex crises, expose NC3 system vulnerabilities, and reinforce human oversight in AI-assisted decision environments.

As nuclear deterrence and decision-making increasingly intersect with a range of EDTs including autonomous weapons, drones, counterspace capabilities, cyber, AI, deepfakes, and quantum computing, they can provide some benefit, but they can also amplify technological complexity and increase nuclear pressures.[10] To navigate this evolving landscape, it is beneficial for decision-makers to incorporate data-driven insights generated by digital twins into their risk assessments and international security dialogues. Establishing and embedding frameworks that ensure their responsible use, prevent misuse for offensive purposes, and promote transparency in nuclear governance is essential for mitigating emerging nuclear risks.

Large-scale digital twin models could provide data that enhances decision-makers' ability to reduce nuclear pressures, navigate complex crises, expose NC3 system vulnerabilities, and reinforce human oversight in AI-assisted decision environments.

Why nuclear risk analysis contains several limitations

Unlike domains such as aviation or cybersecurity, where analysis of large datasets enables risk mitigation, nuclear risk analysis faces several fundamental limitations, including the scarcity of empirical data and methodological challenges in research design. Although academics and analysts acknowledge the significance of nuclear crises, there is little consensus on the dynamics that underpin them.[11] These challenges often lead to disputes over coding, difficulties in determining the appropriate unit of observation, disagreement on the rarity of nuclear crises, and obstacles in drawing meaningful comparisons across cases.[12] Collectively, these factors hinder our ability to reach robust and conclusive insights.[13] A key challenge lies in in determining whether a crisis is characterised by deterrence failures, escalation risks, or both.[14] Some near misses, such as technical errors or false alarms, may not qualify as 'crises', while other cases involve implicit threats rather than overt nuclear brinkmanship.[15]

Traditional risk assessment methods applied for security, defence, and other high-stake applications struggle to fully understand low-probability, high-impact events due to the lack of historical cases.[16] Probabilistic risk analysis, widely applied in finance and public health, is ill-suited for modelling nuclear brinkmanship, where a single misjudgement can have catastrophic consequences. Moreover, decision-making in nuclear crises is often distorted by cognitive biases, such as a decision-makers' rigid adherence to 'adversary images' — how human bias shapes perceptions despite conflicting evidence — as well as conformity to small group views (groupthink), and susceptibility to misinformation, and structural misperceptions that statistical models cannot adequately capture.[17]

A critical factor complicating nuclear decision-making can arise from threat perceptions that can result in the 'use it or lose it' dilemma where perceived NC3 vulnerabilities pressure states into pre-emptive nuclear use.[18] Ambiguity regarding adversary intentions, especially during heightened alerts, can also amplify risks of inadvertent escalation.[19] The 1983 Soviet False Alarm Incident, where a radar misinterpretation nearly triggered nuclear retaliation, demonstrates how imperfect information and time constraints can drive nuclear risk.[20] To navigate the uncertainties of the emerging strategic environment, where technological complexity can compress warning times, overwhelm human decision-making, and create unpredictable feedback loops, it is essential to develop new technological tools to help lower the risk of nuclear use.

Traditional risk assessment methods applied for security, defence, and other high-stake applications struggle to fully understand low-probability, high-impact events due to the lack of historical cases.

Digital twins: a transformative approach to risk reduction

By detecting early warning indicators, digital twins could help decision-makers anticipate potential crises, evaluate alternative responses, and implement de-escalation strategies before tensions spiral out of control and enter the nuclear level. In addition, digital twins also help replicate past incidents, such as the 1983 Soviet false alarm incident, the 1995 Norwegian rocket incident, and the 1962 Cuban Missile Crisis. Using digital twins for this purpose could help decision-makers test how different variables interact in high-risk situations. More importantly, they allow for counterfactual analysis, asking: would the crisis have escalated differently if one variable — technology, intelligence accuracy, or leadership bias — had been different?

Beyond crisis modelling, digital twins could also provide data that enhances the resilience of NC3 systems, which are increasingly vulnerable to cyber intrusions. By helping to mitigate AI-driven automation errors and system malfunctions, digital twins can anticipate weaknesses and reinforce system stability before real-world disruptions occur. This is crucial in an era where EDTs are rapidly reshaping nuclear security dynamics.

Digital twins also serve as advanced risk reduction training platforms for decision-makers, policymakers, and military leaders, offering immersive, high-fidelity environments that can construct novel crisis scenarios. Unlike traditional war games or tabletop exercises, these simulations dynamically adjust based on real-time data, allowing decision-makers to become more aware of their cognitive limitations, refine de-escalation strategies, and improve situational awareness under extreme conditions. In defence contexts, it has been demonstrated that digital twins provide significant informational superiority through improved human-machine teaming.[21] By enhancing experiential learning and equipping policymakers with a deeper understanding of escalation risks, digital twins help bridge the gap between theoretical deterrence models and the unpredictable realities of nuclear crisis management in an evolving EDT landscape.

Digital twins help bridge the gap between theoretical deterrence models and the unpredictable realities of nuclear crisis management in an evolving EDT landscape.

Why now?

The growing complexity of nuclear deterrence and decision-making, amplified by the cumulative effects of EDTs, creates dimensions of complexity that can impinge on the nuclear domain.[22] This necessitates a shift toward simulation-based approaches to identify vulnerabilities and mitigate risks effectively. In this context, several technological shifts are reshaping nuclear risk landscapes, such as:

Artificial intelligence and automation bias: the rapid integration of AI into nuclear intelligence and early warning systems has introduced both opportunities and significant risks. AI-driven decision-support systems can enhance threat detection by rapidly processing vast amounts of intelligence data, identifying patterns, and predicting potential threats with greater speed and efficiency than human analysts alone.[23] However, while AI can support nuclear decision-making, it also introduces automation bias, which includes the tendency of human operators to over-rely on algorithmic recommendations without critically assessing their validity.[24] This overconfidence in AI-generated assessments can erode human oversight, particularly in high-stakes scenarios where rapid decisions are required under immense pressure. A critical danger arises when AI-generated threat assessments are misinterpreted as definitive intelligence, rather than as one input among many. In situations where AI models identify false positives — such as misclassifying routine military exercises as aggressive manoeuvres — decision-makers may be pressured to escalate their response based on incomplete or misleading data.[25]

This challenge is exacerbated by the inherent opacity of some AI models, particularly deep learning-based systems, which function as 'black boxes' that do not always provide clear explanations for their outputs.[26] If policymakers lack an understanding of how AI reaches its conclusions, they may struggle to distinguish between legitimate threats and erroneous alerts, increasing the likelihood of miscalculated responses that escalate rapidly to the nuclear level.[27] In nuclear crisis scenarios, where decision windows are measured in minutes rather than hours, the reliance on AI-driven recommendations without sufficient human verification can result in hasty and irreversible escalation. AI's potential to generate deceptive but plausible false alarms also raises concerns about adversaries deliberately exploiting AI vulnerabilities to provoke miscalculation.[28]

The integration of AI into nuclear decision-making must therefore be approached with extreme caution, ensuring that human oversight remains central and that AI systems are rigorously tested in realistic, high-stakes simulations before being deployed in live environments. Digital twins provide a route to simulate the impact of AI on nuclear decision-making. By modelling real-time AI-generated threat assessments, digital twins allow policymakers to evaluate the accuracy, reliability, and escalation risks associated with AI-driven automation. This enables decision-makers to stress-test AI-driven intelligence frameworks, ensuring that nuclear warning and response protocols remain transparent, verifiable, and resistant to automation bias.

By modelling real-time AI-generated threat assessments, digital twins allow policymakers to evaluate the accuracy, reliability, and escalation risks associated with AI-driven automation

Cyber threats and NC3 vulnerabilities: modern nuclear warning systems rely on a vast and highly interconnected infrastructure that facilitates intelligence gathering, early warning detection, command and control functions, and secure communication between

decision-makers. While these digital systems enhance situational awareness and operational efficiency, they also introduce significant vulnerabilities to cyber intrusions, misinformation campaigns, and system manipulations that can undermine nuclear security and strategic stability.[29]

The growing sophistication of cyber warfare tactics, combined with an increased reliance on automated decision-support tools, raises the risk of misinterpretation, deception, and unintended escalation in nuclear crises. A targeted cyber intrusion into an NC3 system could have multiple destabilising effects.[30] Attackers could manipulate early warning systems to indicate an incoming nuclear strike, leading a state to misinterpret the threat environment and potentially launch a retaliatory response based on incorrect data.[31] This scenario is particularly concerning in high-alert situations, where decision windows are compressed, and leaders must act quickly with incomplete or ambiguous intelligence. A cyber-induced false positive could lead to pre-emptive escalation, while a cyber-induced false negative — in which a real attack is masked — could paralyse a state's ability to respond effectively, undermining deterrence and strategic stability.[32]

Beyond manipulating warning signals, cyber operations could disrupt communication channels between military leaders, policymakers, and field operators, preventing or delaying critical decision-making. This form of network sabotage could be particularly devastating during a crisis, creating confusion about the legitimacy of nuclear orders and increasing the risk of unauthorised or accidental use of nuclear weapons. Adversaries could also deploy misinformation campaigns, for instance by embedding false intelligence into classified systems, misleading decision-makers into believing that a rival is preparing for a nuclear first strike when no such action is actually taking place.[33]

Given the deep-rooted mistrust that often characterises nuclear-armed rivalries, even a minor cyber disruption could trigger a cascade of misperceptions and reactionary policies that push a crisis toward unintended escalation. The increasing integration of AI-driven automation into NC3 decision-support frameworks compounds these risks.[34] While AI can help process vast amounts of intelligence data at unprecedented speeds, cyber adversaries could manipulate AI models by injecting adversarial data, misleading automated systems into misidentifying threats.[35] A cyberattack targeting AI-powered early warning systems could exploit biases in machine learning models, causing them to misclassify benign activities as hostile actions, potentially triggering unnecessary retaliatory measures. This interaction between cyber threats and AI-driven nuclear decision-making represents an emerging and poorly understood risk that requires urgent policy attention.

Digital twins create high-fidelity virtual models of nuclear command networks, enabling real-time simulations of cyberattacks and their potential effects on early warning detection, strategic communications, and response protocols.

To mitigate these threats, digital twins offer a critical tool for testing and enhancing cyber resilience within NC3 systems. Digital twins create high-fidelity virtual models of nuclear command networks, enabling real-time simulations of cyberattacks and their potential effects on early warning detection, strategic communications, and response protocols. By replicating the operational dynamics of NC3 infrastructures, digital twins allow defence planners to identify vulnerabilities, anticipate the impact of cyber disruptions, and refine mitigation strategies before real-world crises occur.

Additionally, digital twins can be used to simulate cyber deception campaigns, helping policymakers understand how misinformation might spread through nuclear intelligence networks and how to design countermeasures to filter out false data.[36] These simulations provide an opportunity to stress-test crisis communication protocols, ensuring that decision-makers have verified channels to confirm or debunk conflicting intelligence during a cyber-induced disruption.

The ability to anticipate, test, and refine defensive strategies against cyber threats in a controlled virtual environment is essential as cyber capabilities continue to evolve. Given that NC3 systems are among the most sensitive and consequential digital infrastructures in existence, policymakers should prioritise cyber resilience by leveraging digital twins to strengthen nuclear security, enhance crisis stability, and reduce the risk of catastrophic decision-making errors.

Quantum computing and cryptographic risks: beyond AI and cyber threats, quantum computing presents a long-term challenge to nuclear security, particularly in the realm of cryptographic safeguards. NC3 systems rely on encrypted communications to maintain the confidentiality and integrity of command structures, ensuring that nuclear orders are both secure and verifiable.[37] These encryption protocols form a critical defence against cyber threats, preventing adversaries from intercepting, tampering with, or spoofing sensitive communications. However, as quantum computing advances, existing encryption methods, particularly public key cryptographic systems, are becoming increasingly vulnerable.[38]

Quantum algorithms, such as Shor's algorithm, have the theoretical ability to break widely used encryption protocols, potentially rendering much of today's nuclear communications infrastructure obsolete.[39] If an adversary were to gain access to quantum decryption capabilities before a state had transitioned to quantum-resistant encryption, secure nuclear communications could be compromised, allowing an adversary to intercept, alter, or fabricate nuclear command messages.[40] The implications of quantum-driven decryption are profound. If a state believes its nuclear launch commands, retaliatory response plans, or second-strike capabilities have been compromised, it may feel compelled to pre-emptively alter its deterrence posture, thereby decreasing crisis stability. Additionally, the inability to trust the authenticity of nuclear orders could paralyse decision-making during a crisis, creating dangerous uncertainty about whether an attack is genuine or the result of a manipulated communication signal.

The transition to quantum-secure encryption is therefore not just a technological necessity, it is a strategic imperative for maintaining the integrity and credibility of nuclear deterrence in the coming decades. Digital twins offer a promising solution by providing a controlled environment to simulate quantum threats, allowing policymakers and defence analysts to test the resilience of cryptographic protocols against quantum-enabled adversaries. By integrating quantum risk assessments into dynamic decision models, digital twins can help governments identify the optimal timeline for transitioning to post-quantum cryptographic standards, reducing the risk of vulnerability gaps during the transition period.

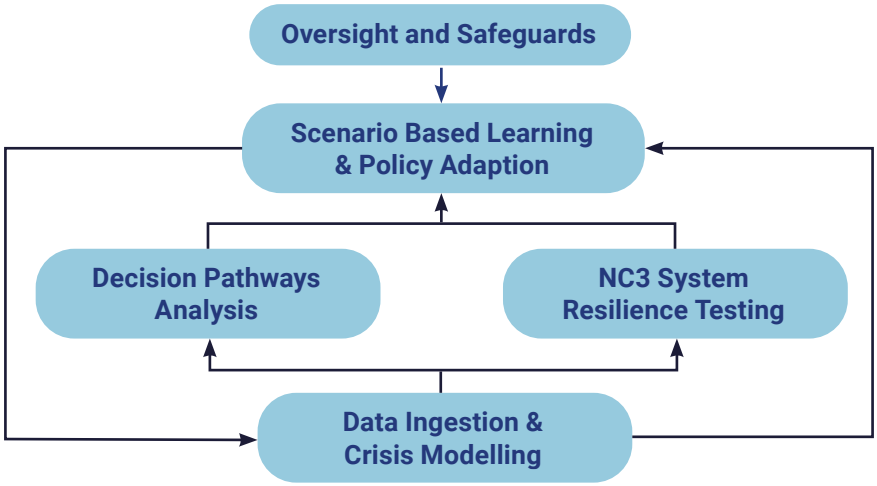
Digital twins can be used to simulate cyber deception campaigns, helping policymakers understand how misinformation might spread through nuclear intelligence networks and how to design countermeasures to filter out false data.

Furthermore, by simulating quantum-enhanced cyberattacks on NC3 infrastructure, digital twins enable policymakers to explore countermeasures, assess failure points, and ensure that nuclear command structures remain secure as cryptographic technology evolves. Proactive preparation in this domain is critical; waiting until quantum threats become fully operational could leave nuclear command systems dangerously exposed. By leveraging digital twins to stress-test nuclear security in a post-quantum world, policymakers can ensure the continued credibility of nuclear deterrence and maintain strategic stability in an era of unprecedented technological change.

By simulating quantum-enhanced cyberattacks on NC3 infrastructure, digital twins enable policymakers to explore countermeasures, assess failure points, and ensure that nuclear command structures remain secure as cryptographic technology evolves.

Key components of a proposed digital twin nuclear decision framework

To integrate digital twins effectively into the nuclear security frameworks of NWS, a structured approach is required. The proposed Digital Twin Nuclear Decision Framework (DT-NDF) outlines how digital twins can be systematically applied to crisis simulation, decision modelling, and NC3 risk assessment.[41]



The Digital Twin Nuclear Decision Framework (DT-NDF) provides a structured, data-driven approach to risk reduction by integrating real-time crisis simulations, NC3 resilience testing, decision pathway analysis, and adaptive learning.

At its foundation, ***Data Ingestion & Crisis Modelling*** enables the continuous integration of geopolitical intelligence, AI-driven escalation analysis, and historical crisis replication. This real-time modelling provides decision-makers with up-to-date insights into emerging threats.

NC3 System Resilience Testing ensures that NC3 infrastructures can withstand cyber intrusions, misinformation attacks, and quantum security risks. By simulating potential system failures, the framework strengthens response strategies. The GSA Framework can be incorporated at this level to assess its effectiveness in mitigating the risks associated with the cumulative impact of EDTs.

Decision Pathway Analysis addresses human factors in nuclear decision-making, identifying cognitive biases, external pressures, and adversary misperceptions. This layer enhances policymakers' ability to assess escalation risks and prevent miscalculated responses.

Scenario-Based Learning & Policy Adaptation provides an iterative environment where nuclear policymakers can test strategies, refine AI-assisted decision trees, and adjust policies based on live geopolitical shifts.

Finally, ***Oversight & Safeguards*** ensure that digital twin models remain transparent, accountable, and aligned with international nuclear governance norms, preventing their misuse for offensive strategies or automated escalation.

The *Digital Twin Nuclear Decision Framework* (DT-NDF) provides a structured, data-driven approach to risk reduction by integrating real-time crisis simulations, NC3 resilience testing, decision pathway analysis, and adaptive learning.

Digital twins for nuclear risk reduction: sector specific regulation

The use of digital twins in the nuclear weapons risk reduction domain requires the consideration of relevant existing governance frameworks, substantive laws and regulations, and normative ethical principles.

Digital twin regulations consist of sector and use case-specific guidelines. A dominant example of this is in the healthcare sector where there are numerous governance initiatives, such as the European Medicines Agency (EMAs) guidelines for the use of digital technologies, including digital twins, in clinical trials.[42]

While Europe does not have specific guidelines of direct applicability to nuclear decision-making, the U.S. Nuclear Regulatory Commission (NRC) has developed guidelines for digital technologies, including digital twins, for this sector. The NRC guidelines are not applicable to all potential uses of digital twins but are instead dependent on whether the digital twin is to be used as a control system, a protection system, or as input to determining safety system settings. Here, the applicable provisions for each use category draws from requirements of standards organisations such as the Institute of Electrical and Electronics Engineers (IEEE) (CR 50.55a), from the use of licensing regimes (CR 50.59) and from design certification requirements (CR 52.47) amongst others.[43]

Nevertheless, digital twins for nuclear decision-making in the EU should keep cognisant of the broader safety and security provisions stipulated in the Euratom Treaty, the Nuclear Safety Directive, and the Nuclear Energy Agency (NEA).

The use of digital twins in the nuclear weapons risk reduction domain requires the consideration of relevant existing governance frameworks, substantive laws and regulations, and normative ethical principles.

Aligning digital twins with international safeguards

The integration of digital twins as a risk reduction mechanism by the NWS must be guided by international norms and principles on the responsible use of AI to prevent misuse or unintended consequences. These considerations include:

i. Transparency in AI-assisted decision-making: AI-driven decision support must remain interpretable and accountable, ensuring that digital twin-generated intelligence is auditable, bias-resistant, and aligned with human oversight requirements.

ii.Preventing misuse: one risk of digital twin simulations is their potential weaponisation. They could, for instance, be used to justify preventative or pre-emptive nuclear attacks by simulating adversary escalation under biased assumptions. Strict verification protocols and multilateral oversight can mitigate these risks.

iii. Ensuring secure and tamper-proof digital twin models: since digital twins store sensitive intelligence and strategic insights, their cybersecurity needs to be as robust as NC3 systems themselves. Quantum-secured encryption and redundant verification layers will be necessary to prevent adversarial tampering. These issues may be alleviated by using twins offline (on device).

The integration of digital twins as a risk reduction mechanism by the NWS must be guided by international norms and principles on the responsible use of AI to prevent misuse or unintended consequences.

References

1 Belen Bianco and Rishi Paul, "Technological Complexity and Risk Reduction: A Guardrails and Self-Assessment Framework for EDTS in NC3 and Nuclear Weapons Decision-Making", (ELN, July 2024)

2 Graham Kenny and Ganna Pogrebna, "Digital twins can help you make better strategic decisions" (Harvard Business Review, September 23, 2024). https://hbr.org/2024/09/digital-twins-can-help-you-make-better-strategic-decisions

3 United Nations, "A Nuclear Risk Reduction Package, p. 4", (Working paper submitted by the Stockholm Initiative, to the 2020 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, UN document NPT/CONF.2020/WP.9/Rev.1, 2022), https://www.government.se/contentassets/69558f7f0bbc48c0ad2a2c0e70e7ca9a/working-paper---a-nuclear-risk-reduction-package.pdf

4 Ryan Chan, "China hosts nuclear weapons talks amid saber-rattling in Europe", (Newsweek, World, 11th December 2024), https://www.newsweek.com/china-news-hosts-nuclear-weapons-talks-amid-saber-rattling-europe-1999125

5 United Nations, "2020 Review Conference of the States Parties to the Treaty on the Non-Proliferation of Nuclear Weapons; Working paper of the President Final Document". (August 26, 2022). Available at: https://digitallibrary.un.org/record/3986171?ln=en&v=pdf

6 United Nations, "2020 Review Conference of the States Parties to the Treaty on the Non-Proliferation of nuclear Weapons; Draft Final Document". (August 25, 2022). Available at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2022/documents/CRP1_Rev2.pdf

7 The DT-NDF offers a structured, data-driven approach to risk reduction by combining real-time crisis simulations, NC3 resilience testing, decision pathway analysis, and adaptive learning. See section entitled "Key Components of a Proposed Digital Twin Nuclear Decision Framework" for more information.

8 For more information on digital twins, see: "What is a digital twin?" (IBM, 05 August 2021), https://www.ibm.com/think/topics/what-is-a-digital-twin

9 The baseline prototype developed by the ELN and AICF focused on three key EDTs: offensive cyber capabilities, artificial intelligence, and deepfakes.

10 For more reading on the aggregate risks posed by EDTS to nuclear NC3 systems, see: Bianco and Paul, (July 2024).

11 Mark S. Bell and Julia Macdonald, "How to Think About Nuclear Crises", p. 43 (Texas National Security Review, Volume 2, February 2019). http://dx.doi.org/10.26153/tsw/1944

12 See, for example, James Fearon, "Selection Effects and Deterrence", pp. 5 – 29 (International Interactions 28, no. 1, 2002) https://www.tandfonline.com/doi/abs/10.1080/03050620210390

13 Francis J. Gavin, "Nuclear Weapons and American Grand Strategy", pp. 67 – 69, (The Brookings Institution: Washington: D.C, 2020). https://www.brookings.edu/books/nuclear-weapons-and-american-grand-strategy/

14 Fearon, James, (2002), pp. 5 – 29.

15 Francis J. Gavin, (2020), pp. 67 – 69.

16 Ganna Pogrebna and Mark Skilton, "Navigating new cyber risks: how businesses can plan, build and manage safe spaces in the digital age" (Springer International Publishing, 2019). https://link.springer.com/book/10.1007/978-3-030-13527-0; Joakim Sundh, "Human behavior in the context of low-probability high-impact events", (Humanities and Social Sciences Communications 11, 902, 2024). https://doi.org/10.1057/s41599-024-03403-9

17 Bruce Russet, "The Prisoners of Insecurity: Nuclear Deterrence, The Arms Race, And Arms Control", pp. 120-132, (W.H. Freeman and Company, San Francisco, 1983). For the effects of the spiral model on perceptions, see also: Robert Jervis, "Perception and Misperception in International Politics" (Princeton University Press, 1976); Atsuo Murata, Tomoko Nakamura, and Waldemar Karwowski, "Influence of cognitive biases in distorting decision making and leading to critical unfavourable incidents", pp. 44 - 58, (Safety, 1(1), 2015). https://www.researchgate.net/publication/283760470_Influence_of_Cognitive_Biases_in_Distorting_Decision_Making_and_Leading_to_Critical_Unfavorable_Incidents

18 Bianco and Paul (July 2024).

19 Barry R. Posen, "Inadvertent Escalation: Conventional War and Nuclear Risks", (Cornell University Press, US, 1991).

20 For further reading of this incident, see: Taylor Dowling, "1983: The World at the Brink" (Little, Brown Book Group, UK, 2018).

21 Kapish Aggarwal, et. al. "Enabling Elements of Simulations Digital Twins and its Applicability for Information Superiority in Defence Domain" (Paper presented at Modelling and & Simulation Group (NMSG) Symposium, STO-MP-MSG-197, Bath, United Kingdom, 29 September 2022) doi:10.14339/STO-MP-MSG-197

22 Bianco and Paul (July 2024).

23 James Johnson, "AI and the Bomb", (Oxford University Press, Croydon, UK, 2023).

24 Michael Depp and Paul Scharre, "Artificial Intelligence and Nuclear Stability", (War on the Rocks, 16 January, 2024), https://warontherocks.com/2024/01/artificial-intelligence-and-nuclear-stability/; Saar Alon-Barkat, Madalina Busuioc, "Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice", pp. 153 – 169, (Journal of Public Administration Research and Theory, Volume 33, Issue 1, January 2023), https://doi.org/10.1093/jopart/muac007.

25 Bianco and Paul (July 2024).

26 Johnson, James, (2023), pp. 17-18.

27 Natasha E. Bajema, and John Gower, "A Handbook for Nuclear Decision-Making and Risk Reduction in an Era of Technological Complexity". Edited by Francesco Femia. (Washington, DC: The Janne E. Nolan Center on Strategic Weapons, an institute of The Council on Strategic Risks, December 2022). https://councilonstrategicrisks.org/analysis/reports/nuclear-decision-making-and-risk-reduction-in-an-era-of-technological-complexity/.

28 Bianco and Paul (July 2024).

29 Bajema, and Gower (2022).

30 Jake Hecla, Rebecca Krentz-Wee, and Andrew Reddie, "The Next Generation NC3 Enterprise: Opportunities and Challenges" (United States). https://www.osti.gov/servlets/purl/1614797.

31 Page O Stoutland and Samantha Pitts-Kiefer, "Nuclear Weapons in: 'The New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group', (NTI, September 2018), https://www.nti.org/wp-content/uploads/2018/09/Cyber_report_finalsmall_Zg5TarX.pdf

32 Ibid.

33 Ibid.

34 Johnson, James, (2023).

35 Andrew Lohn, "Hacking AI: A Primer for Policymakers on Machine Learning Cybersecurity', Centre for Security and Emerging Technology", p. 5, (December 2020). https://cset.georgetown.edu/publication/hacking-ai/

36 Jessica Heluany, Ahmed Amro, Vasileios Gkioulos, and Sokratis Katsikas, "Interplay of Digital Twins and Cyber Deception: Unravelling Paths for Technological Advancements'. In "Proceedings of the 2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability", pp. 20–28. (New York, NY: Association for Computing Machinery, 2024). https://doi.org/10.1145/3643662.3643955.

37 Dominic Rosch-Grace and Jeremy Straub, "Analysis of the Likelihood of Quantum Computing Proliferation" (Technology in Society 68, 2022): 101880, https://doi.org/10.1016/j.techsoc.2022.101880.

38 Travis Scholten, et. al "Assessing the Benefits and Risks of Quantum Computers" (IEEE Security & Privacy, 2024). https://www.nist.gov/publications/assessing-benefits-and-risks-quantum-computers

39 For more information on Shor's algorithm see: Hiu Yung Wong, "Shor's Algorithm" In "Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps", pp. 289–298. (Cham: Springer International Publishing, 2024), https://doi.org/10.1007/978-3-031-36985-8_29.

40 Jake Tibbetts, "Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers," (2019), https://doi.org/10.2172/1566798; Andy Majot and Roman Yampolskiy, "Global Catastrophic Risk and Security Implications of Quantum Computers", pp.17-26, (Futures 72, 2015). https://doi.org/10.1016/j.futures.2015.02.006.

41 Ganna Pogrebna, Rishi Paul, Nathan Damaj, Jake McNaughton, Graham Stacey and Immaculate-Motsi OmoijiWWade, April 2024.

42 "Multi-annual AI workplan 2023-2028', HMA-EMA Big Data Steering Group, Version 1" (November 2023). https://www.ema.europa.eu/en/documents/work-programme/multi-annual-artificial-intelligence-workplan-2023-2028-hma-ema-joint-big-data-steering-group_en.pdf

43 "10CFR50.55a Codes and Standards", (Modified by Final Rules, 17, January, 2018), http://www.inserviceengineering.com/uploads/6/7/3/8/6738112/10cfr50.55a_[1-1-2018]_formatted_by_inservice_engineering.pdf; "1786-2022 - IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities", (Redline, IEEE, New York, 2022). https://ieeexplore.ieee.org/document/9927292; "52.47 'Contents of applications; technical information'", (U.S. Nuclear Regulatory Commission), https://www.nrc.gov/reading-rm/doc-collections/cfr/part052/part052-0047.html

The European Leadership Network (ELN) is an independent, non-partisan, pan-European network of over 450 past, present and future European leaders working to provide practical real-world solutions to political and security challenges.

Contact

For further information on the ideas in this report, please contact secretariat@europeanleadershipnetwork.org

Published by the European Leadership Network, April 2025

European Leadership Network (ELN)
8 St James's Square
London, UK, SE1Y 4JU

@theELN | europeanleadershipnetwork.org

European Leadership Network
8 St James's Square
London, SW1Y 4JU
United Kingdom

Email: secretariat@europeanleadershipnetwork.org
Tel: 0203 176 2555

Follow us

europeanleadershipnetwork.org