Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Juan de Dios Meseguer González
PhD candidate in International Security at IUGM-UNED

Email: jmeseguer1@alumno.uned.es

Analysis of Cyber Risks and Resilience in the Russian Nuclear Triad

Abstract

This paper studies the technological exposure and resilience of Russia's nuclear command, control and communications (NC3) system in the context of global strategic competition and emerging security challenges in the Euro-Atlantic space. It proposes a reproducible methodological model that combines systematic review, conceptual analysis of command and control architectures, and scenario simulation based on NIST 800-30 and ISO/IEC 27005 standards.

The research uses open and validated scientific intelligence (OSINT) from institutional sources such as RAND, NATO STO and SIPRI, transforming the absence of classified data into an opportunity to establish a verifiable analytical basis. From an interdisciplinary perspective, mitigation frameworks and improvement measures are proposed based on Zero Trust architectures, cyber-resilience audit processes, and strategic information cross-verification mechanisms.

The study provides a reference framework for understanding and assessing the effects of military digitalisation on contemporary strategic stability, offering a useful tool for researchers and defence officials interested in strengthening international technological security.

Keywords

Strategic security, Cyber defence, Command and control systems, Technological deterrence, Euro-Atlantic cooperation.

Cite this article:

Meseguer Gonzalez, J. D. (2025). Analysis of cyber risks and resilience in the Russian nuclear triad. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 343-382.

1 Introduction

Cyber risk in strategic nuclear command, control and communications (NC3) systems has become a critical factor for international stability. The progressive digitisation of launch vectors, the automation of early warning protocols and the integration of artificial intelligence into strategic decision-making processes have increased exposure to cyberattacks or interference. In this context, the Russian nuclear triad—consisting of land-based intercontinental missiles, missile-launching submarines, and strategic air platforms—represents one of the most sensitive environments for global deterrence balance.

The tensions arising from the conflict in Ukraine since 2022 and NATO's adaptive response have substantially altered the Euro-Atlantic strategic environment. Russia has prioritised the strengthening of its nuclear deterrence and has invested in the modernisation of its NC3 network, integrating cyber and artificial intelligence capabilities into its warning and command systems. At the same time, the Atlantic Alliance has accelerated its advanced cyber defence doctrine, creating coordination structures such as the *NATO CyOC* (Cyber Operations Centre) and expanding interoperability programmes between member states.

In this scenario of technological rivalry, understanding the cyber risks associated with the Russian nuclear triad becomes a fundamental task for international security, especially from a preventive and doctrinal point of view. The scarcity of public information on these systems, coupled with the secretive nature of most command and control infrastructures, necessitates the adoption of alternative methodologies based on verified open sources (OSINT), recognised risk frameworks such as NIST 800-30 and ISO/IEC 27005, and modelling techniques that allow theoretical behaviours to be extrapolated without compromising classified information.

In this regard, this paper does not seek to identify specific vulnerabilities or describe specific technical structures, but rather to offer a reproducible methodological model for analysing cyber risk and doctrinal resilience in critical nuclear command infrastructures. This approach allows the phenomenon to be approached from a scientific, auditable and practical perspective for academic institutions, strategic think tanks and defence agencies operating in restricted information environments.

The novelty of the research lies in three main aspects:

1. The systematic application of the NIST 800-30 framework to a domain traditionally reserved for classified intelligence.
2. The incorporation of the concept of strategic resilience, understood not only as the ability to withstand a cyberattack, but also to maintain doctrinal and operational stability in a hostile digital environment.
3. The formulation of an open, verifiable and replicable analytical model that allows for future interdisciplinary research without compromising information security.

Ultimately, this study seeks to contribute to the debate on deterrent stability in the digital age by proposing a conceptual and methodological framework that facilitates scientific and technological cooperation among allies and fosters a culture of prevention, deterrence and response to new-generation technological threats.

The following section describes the methodology adopted, the document selection criteria and the thematic coding process applied to construct the analysis model.

2 Methodological framework and sources

The study is based on a rigorous methodology designed to ensure the scientific validity of the analysis without violating security restrictions or revealing classified information. Given that the research addresses a highly sensitive area—the Russian nuclear command, control and communications (NC3) system—a mixed and reproducible method was chosen that combines systematic literature review, thematic coding and risk scenario modelling under international cyber management standards. This approach allows for the development of a verifiable analytical framework based on open sources, structured in phases ranging from document selection to methodological validation of the model.

2.1 General approach

This study adopts a mixed qualitative-quantitative approach aimed at analysing cyber risk in strategic nuclear command, control and communications (NC3) infrastructures. Given the confidential nature of the subject matter, a methodology based on the triangulation of verified open sources, international risk management frameworks and conceptual inference techniques is used.

Before developing each phase, the methodological process followed is summarised in table I, which shows the sequence of analysis and the reference standards applied.

TABLE I. METHODOLOGICAL PHASES AND REFERENCE FRAMEWORKS APPLIED

Phase	Analytical objective	Tool/Reference	Expected result
1 Systematic document review	Identify institutional and academic literature on NC3, cybersecurity and strategic resilience (2018-2025).	PRISMA 2020 protocol. Sources: RAND, NATO STO, SIPRI, IISS, Chatham House.	Verified corpus of open sources (58 documents).
2 Thematic coding	Group findings into three areas: structural vulnerability, strategic digitalisation and doctrinal response.	Inductive content analysis.	Risk and resilience indicator matrix.
3 Risk scenario modelling	Simulate possible vectors of interference or degradation of the NC3 from a theoretical point of view.	NIST SP 800-30 Rev. 1 (2012); ISO/IEC 27005 (2018).	Conceptual exposure and resilience scenarios.
4 Strategic impact assessment	Assess the potential impact on deterrent stability and Euro-Atlantic cooperation.	Semi-quantitative scale (probability × impact).	Strategic risk map (theoretical).
5 Synthesis and methodological validation	Verify the consistency of the model with allied cyber defence doctrine.	Cross-check RAND–NATO STO–SIPRI.	Reproducible and auditable methodological framework.

Source: author's own elaboration based on NIST 800-30 (2012) and ISO/IEC 27005 (2018).

2.2 Selection and validation of the document corpus

The initial empirical base consisted of 312 documents obtained from institutional databases and specialised think tanks—including RAND (*Research and Development Corporation*), SIPRI (*Stockholm International Peace Research Institute*), NATO STO (*Science and Technology Organisation*), CSIS (*Centre for Strategic and International Studies*), IISS (*International Institute for Strategic Studies*), Chatham House, and Carnegie Endowment—selected for their relevance and analytical rigour. After applying criteria of thematic relevance, institutional authenticity, and absence of duplicates, the corpus was reduced to 58 main references.

The PRISMA 2020 protocol (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), an international guideline for the transparent and reproducible preparation of systematic reviews, was used to refine the sources and ensure their methodological traceability. Subsequently, inductive thematic coding was applied, which allowed the findings to be grouped into three areas of analysis:

a) Structural vulnerabilities of NC3;

b) risks arising from strategic digitalisation and artificial intelligence;

c) doctrinal responses and resilience frameworks in the Euro-Atlantic environment.

Each document was recorded in a documentary annex with verified URLs and basic metadata (author, year, institutional source, type of document), ensuring the verifiability and reproducibility of the process.

The sources used were classified into four main categories:

1. Doctrinal and technical documents issued by international organisations (NATO, UN, European Union, Ministry of Defence of the Russian Federation).
2. Reports from think tanks and strategic research organisations (RAND, NATO STO, SIPRI, IISS, Chatham House).
3. Academic and scientific literature indexed in databases such as Scopus, Web of Science, and Dialnet Plus.
4. Verified journalistic sources, used only to contextualise recent developments (2022–2025) in missile modernisation and command doctrines.

The authenticity of each document was verified by cross-checking its institutional origin, date of issue, bibliographic citation and public availability. This validation ensures that the OSINT sources used meet criteria of traceability, timeliness and reliability, complying with the standards of transparency required by scientific research in the field of defence.

2.3 Application of the NIST 800-30 and ISO/IEC 27005 models

The risk analysis followed the structure proposed by the NIST SP 800-30 guide (*Guide for Conducting Risk Assessments*, developed by the US *National Institute of Standards and Technology*), adapted to the strategic defence context. This framework

provides a standardised procedure for identifying, estimating and prioritising technological risks in critical systems:

1. Identification of critical NC3 assets and functions (without detailing platforms or protocols).
2. Characterisation of threats according to cyber typology: communications interference, software sabotage, sensor manipulation and cognitive disinformation.
3. Estimation of the probability and impact of each threat on strategic stability using a semi-quantitative scale.
4. Determination of residual risk and formulation of mitigation strategies.

In addition, the ISO/IEC 27005 standard, issued by the *International Organisation for Standardisation* and the *International Electrotechnical Commission*, was applied, which provides guidelines for information security risk management. Its integration allows the organisational and doctrinal dimension of resilience to be incorporated, aligning technical analysis with the principles of governance and operational control. The result is a reproducible model for strategic cyber risk analysis, applicable to critical infrastructures with limited access to classified information.

2.4 Justification for the use of open sources (OSINT)

Far from being a limitation, reliance on open sources represents a methodological advantage in terms of transparency, security, and scientific cooperation. The use of OSINT allows for:

– Validate hypotheses using verifiable and accessible information;
– Respect operational confidentiality margins;
– Promote academic and doctrinal collaboration between allies.

In this way, information restriction becomes a legitimate epistemological condition, where innovation focuses on the analysis model, not on the disclosure of sensitive data. Thus, the study contributes to consolidating a common methodological language for the examination of cyber risk in strategic environments and for interaction between academia and defence institutions.

2.5 Limitations and future prospects

It is recognised that the exclusive use of OSINT prevents direct empirical verification with classified data. However, the model developed can be extended and validated by researchers with restricted access, ensuring its scalability.

Future lines of research include the application of machine learning to detect risk patterns and the comparative analysis of cyber resilience between NC3 doctrines of different nuclear powers.

Taken together, this methodological framework provides a scientific and reproducible basis for future studies on strategic cybersecurity and resilience in nuclear command systems.

3 Theoretical and conceptual framework

Understanding cyber risk in the Russian nuclear triad requires articulating a theoretical basis that combines classic doctrinal approaches to deterrence with new paradigms of digital security and technological resilience. This section establishes the *conceptual foundations* that underpin the subsequent analysis, integrating contributions from academic literature, strategic research reports and international regulatory frameworks on cyber risk management (ISO/IEC, 2022; Joint Task Force, 2018).

The purpose of this framework is not to reveal specific command structures, but to offer an interpretative model that allows us to understand how the digitalisation of the Russian NC3 system can affect global strategic stability. From this perspective, deterrence theory, nuclear risk studies and doctrinal developments in cyber defence converge to explain a changing scenario, where technological risk becomes a geopolitical vector of the first order (Johnson, 2021; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

The purpose of this framework is not to reveal specific command structures, but to offer an interpretative model that allows us to understand *how the digitalisation of Russia's NC3 system can affect global strategic stability.* From this perspective, deterrence theory, nuclear risk studies and doctrinal developments in cyber defence converge to explain a changing scenario, where technological risk becomes a geopolitical vector of the first order (Johnson, 2021; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

3.1 Fundamentals of the nuclear triad and the NC3 system

The nuclear triad is at the heart of modern strategic deterrence. Designed to ensure second-strike capability, it consists of three complementary components: intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs) and strategic bombers (Kristensen and Korda, 2023). The logic of the triad is to maintain credible deterrence through the survival of the arsenal in the face of a pre-emptive strike, a concept that remains central to current Russian doctrine (IISS, 2023). Comparative data on forces and modernisation programmes support this configuration of the Russian triad (IISS, 2024).

The Nuclear Command, Control and Communications (NC3) system integrates the functions of political command, operational control and transmission of orders to nuclear forces. According to Acton (2018), the reliability of NC3 is the *sine qua non* of global nuclear stability: any degradation or ambiguity in its operation could lead to a crisis of perception or accidental escalation.

The Russian NC3 has evolved from Soviet architecture (*Kazbek System*, *Cheget*) to a more automated network, supported by GLONASS satellites and redundant

encrypted communications (CSIS, 2024; Mazarr *et al.*, 2022). However, digital interconnection and the introduction of artificial intelligence into decision-making processes also increase exposure to interference or cyberattacks (Kristensen and Korda, 2022b).

This technological evolution raises the need to assess the risks associated with the digitisation of NC3. Understanding the nature and dimensions of cyber risk in strategic systems thus becomes the logical next step in interpreting the vulnerabilities inherent in the contemporary deterrence model.

3.2 Cyber risk in strategic systems

Cyber risk is defined as the probability that a digital action or vulnerability will affect the integrity, confidentiality or availability of a critical system (Joint Task Force, 2018). In the nuclear domain, this risk transcends the technical realm: it can alter trust between states and destabilise deterrence balances.

Studies by the *Carnegie Endowment for International Peace* and *SIPRI* highlight that cyber incidents in strategic infrastructure can generate 'catalytic effects', i.e. trigger disproportionate reactions due to misperceptions by the adversary (Jung, 2024; Kristensen y Korda, 2022b). Mazarr *et al* (2022) and CSIS (2024) agree that Russian NC3, despite its redundancy, faces increasing risks linked to sensor automation, dependence on proprietary software and remote access to decision nodes.

According to these studies, the main threat vectors fall into four categories:

1. Digital intrusion or firmware manipulation in strategic communication nodes.
2. Electromagnetic or satellite signal interference, which affects the reliability of early warning.
3. Disinformation and cyber deception operations targeting the political-military chain of command.
4. Technological dependence and vulnerability of the supply chain, especially for imported microelectronic components.

These threats, documented in reports by NATO STO *(2023)* and IISS *(2023)*, illustrate how strategic digitalisation transforms classic deterrence risks into multidimensional challenges combining cybersecurity, intelligence and strategic psychology.

Analysis of these risk vectors necessarily leads to an examination of resilience capabilities. If risk represents the degree of exposure, resilience determines the system's ability to maintain its critical functions under attack or disruption. This shift in focus is key to understanding stability in the digital nuclear environment.

3.3 Strategic resilience and cyber stability

The concept of strategic resilience has evolved from a technical notion to a doctrinal principle that defines the ability of states to maintain essential functions under

pressure or attack (Payne, 2022). In the cyber context, it implies not only resisting aggression, but also ensuring operational continuity, organisational adaptability and rapid recovery of the affected system.

NATO formalised this vision after the Warsaw Summit (2016) and reaffirmed it in its *Strategic Concept 2022*, recognising cyberspace as an operational domain. Its *Cyber Defence Pledge* and the research framework of the *NATO Science and Technology Organisation* (U.S. Department of Defense, 2020) promote the integration of digital resilience into defence planning.

Russia, for its part, has been developing a doctrine of 'informational stability' since 2020, which combines cyber defence with information control and technical redundancy of NC3 systems (CSIS, 2024). This vision focuses on maintaining technological autonomy and reducing exposure to external vulnerabilities.

The shift from technical resilience to strategic resilience introduces a new component: *cyber deterrence*. While resilience ensures the survival of the system, deterrence ensures the predictability of the adversary. The two complement each other in a framework where stability depends as much on technological strength as on perceived credibility.

3.4 Cyber deterrence and strategic stability

The digital transformation of nuclear deterrence has led to the emergence of the concept of cyber deterrence, understood as the ability to prevent aggression through robust protection of critical infrastructure and credible responses to attacks (Johnson, 2021).

Authors such as Futter (2018) and Morgan (2023) argue that traditional deterrence—based on the fear of mutually assured destruction—is shifting towards 'resilience deterrence', where the strength of the system and its ability to absorb an attack without losing functionality are decisive factors.

Contemporary strategic stability is therefore defined not only by the quantity or power of the nuclear arsenal, but also by the cyber robustness of the NC3. The RAND (2025) and SIPRI (2024) reports warn that digital vulnerability in nuclear command networks could become the main catalyst for instability if coordinated measures for prevention, cooperation and technological transparency are not adopted among the powers.

This set of concepts—risk, resilience, and cyberdeterrence—forms the basis of the analytical model used in this research. Based on these concepts, an integrative conceptual framework is established that links technological security with strategic stability, serving as a basis for the discussion of results.

3.5 Summary of the conceptual framework

The theoretical framework of this study is based on four fundamental pillars:

1. The nuclear triad, as a classic deterrent structure and guarantor of strategic balance (Kristensen and Korda, 2023).

2. The NC3 system, as the technical and doctrinal core of nuclear communication (Jung, 2024; CSIS, 2024).
3. Cyber risk, which introduces technological and strategic uncertainty (Joint Task Force, 2018; SIPRI, 2024).
4. Strategic resilience, which transforms cybersecurity into an element of stability (Payne, 2022; U.S. Department of Defense, 2020).

These concepts form an integrative framework that allows us to examine the levels of exposure and recovery of Russian NC3 in the context of global technological competition.

Next, a Glossary of Basic Terms and Acronyms (Section 4) is presented to facilitate understanding of the technical, doctrinal, and technological concepts used in the research.

Section 5 then develops the results of the analysis, organised around the three identified axes: structural vulnerability, strategic digitalisation and doctrinal response.

4 Glossary of basic terms and acronyms

This glossary provides concise definitions of the main technical and doctrinal concepts used throughout the article. Its purpose is to facilitate understanding of the specialised terminology related to strategic cybersecurity, nuclear deterrence and command and control systems (NC3), so that the reader does not have to resort to external sources.

The inclusion of this section responds to the reviewers' recommendation to provide an early terminological frame of reference, allowing for a fluid and coherent reading of the subsequent sections. The definitions presented combine technical, doctrinal and scientific criteria and have been drawn from indexed academic literature and recognised institutional sources (Jung, 2024; Futter, 2018; Kristensen and Korda, 2023; Payne, 2022; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

TABLE A. GLOSSARY OF BASIC TERMS AND ACRONYMS

Term/Acronym	Summary academic definition	Application in the study
NC3 (Nuclear Command, Control and Communications)	Set of systems, networks and procedures that enable national authorities to control and communicate orders regarding the use of nuclear weapons.	Functional core of Russian nuclear deterrence analysed in this study.
Nuclear triad	Structure composed of three launch platforms: land-based intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs) and strategic air vectors.	Structural framework for assessing cyber risk in each domain.
ICBM (Intercontinental Ballistic Missile)	Ballistic missile with a range of over 5500 km, capable of carrying nuclear warheads between continents.	One of the three components analysed in the Russian triad.
SLBM (Submarine-Launched Ballistic Missile)	Ballistic missile launched from nuclear-powered submarines, an essential part of second-strike capability.	Represents the naval dimension of Russia's NC3.

Term/Acronym	Summary academic definition	Application in the study
Second strike	A state's ability to respond with nuclear weapons after suffering an initial attack.	A key indicator of strategic stability and the impact of cyber risk.
Cyber deterrence	Strategy aimed at preventing cyber attacks through resilience, attribution and proportional response capability.	Concept used to assess the NATO-Ukraine response to strategic cyber threats.
Cyber resilience	A system's ability to withstand, adapt and recover from a cyber attack while maintaining critical functions.	Operational objective for reinforcement in NC_3 systems.
OSINT (Open Source Intelligence)	Intelligence obtained from open, verifiable and publicly accessible sources, used for strategic or scientific analysis.	Methodological basis that guarantees the transparency and reproducibility of research.
NIST (National Institute of Standards and Technology)	US agency that develops technical and methodological standards, including the Special Publication 800-30 series for risk analysis.	Main methodological reference for cyber risk modelling.
ISO/IEC (International Organisation for Standardisation / International Electrotechnical Commission)	International entities that issue joint standards on information security management and technological risk (ISO/IEC 27005).	Complementary framework to NIST for assessing organisational resilience.
Spoofing	Manipulation or spoofing of electronic signals—especially GNSS or satellite signals—in order to alter navigation or location data.	Technical risk identified in SLBM guidance systems and air vectors.
Firmware	Low-level software that controls hardware operation and provides the interface between equipment and programmes.	Potential attack surface in control and launch systems.
GLONASS	Global satellite navigation system of the Russian Federation, equivalent to GPS.	Critical technological dependency for synchronisation and guidance.
Perimetr	Russian automated command system designed to ensure nuclear retaliation even in the event of loss of communication with political command.	Doctrinal example of automation with inherent cyber risk.
Zero Trust	Security model that eliminates implicit trust within internal networks, verifying each access or transaction.	Recommended principle for modernising Russian and allied NC_3 security.

Source: author's own elaboration based on Jung (2024), Futter (2018), Harknett and Smeets (2020), Kristensen and Korda (2023), Payne (2022), Mazarr *et al* (2022), Joint Task Force (2018), ISO/IEC (2018) and U.S. Department of Defense (2020). The definitions summarise standardised technical terminology in nuclear doctrine and cybersecurity.

This glossary constitutes a conceptual reference that frames the technical and strategic analysis developed in the following sections. By clarifying essential terminology, it seeks to ensure that the reader interprets the doctrinal, technical and operational terms used in the study in a consistent manner.

The following section presents the results and technical analysis derived from the application of the methodological model, organised around the three defined areas of research: structural vulnerability, strategic digitalisation and doctrinal response.

5 Results and technical analysis

The study focused on the three components of Russia's nuclear triad—intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs) and strategic air vectors—examining the interactions between the communication, guidance and control subsystems. This multidimensional approach

made it possible to determine the differential exposure to cyber risk in each operational domain.

Among the systems evaluated, the RS-24 Yars is a paradigmatic case due to its strategic relevance and degree of digitalisation, making it a reference model for understanding the convergence between technology, doctrine and vulnerability.

5.1 The RS-24 Yars as a technical reference model

Before presenting the quantitative results, it is necessary to contextualise the technical model that serves as the basis for the empirical analysis. The RS-24 Yars represents the main land-based vector of the Russian triad and exemplifies the complexity of the digital command and control chains associated with ICBMs.

Figure 1, shown below, illustrates the structural configuration and relevance of the land-based component of the NC3 system, highlighting the criticality of firmware and guidance modules as potential cyber exposure surfaces.

Figure 1. RS-24 Yars intercontinental ballistic missile system.
Note: The RS-24 Yars is the main ICBM in the Russian nuclear triad. Its digital architecture and automated guidance systems highlight the potential vulnerability of firmware and control communication networks.
Source: GlobalSecurity.org (n. d.). RS-24 Yars Intercontinental Ballistic Missile

The RS-24 Yars (PC-24 *'Ярс'*; NATO designation SS-27 Mod 2) is a solid-fuel intercontinental ballistic missile (ICBM) with a range of approximately 12 800 km and multiple MIRV thermonuclear warheads (100-550 kt). In service since 2010, it can be launched from fixed silos or mobile TEL (Transporter-Erector-Launcher) platforms, designed to ensure the mobility and survivability of the system. It is an evolution of the *Topol-M* and was designed to overcome contemporary missile defence systems, incorporating autonomous guidance algorithms and digital redundancy (Kristensen and Korda, 2023; IISS, 2023).

Its integration into digital networks and its reliance on encrypted communication channels make the RS-24 a priority for analysis within the Russian NC3 system. Based on this model, two complementary levels of assessment were developed:

1. Chronological and qualitative analysis (2020-2025): chronology of relevant technological and cyber incidents.
2. NIST 800-30 risk modelling: quantification of relative risk by combining probability (P) and impact (I).

Based on the findings of the qualitative analysis, the verified chronology of technological and cyber incidents (2020-2025) is presented below in order to contextualise the evolution of risk prior to its quantitative modelling.

5.2 Chronology of incidents and vulnerabilities (2020–2025)

The chronology below summarises the relevant incidents associated with technological failures or cyberattacks that potentially affected the Russian NC3. Each record was validated by cross-checking academic sources, think tanks and international organisations (SIPRI, 2024; RAND Corporation, 2021; CSIS, 2024; U.S. Department of Defense, 2020; IISS, 2023).

Following the analysis of the RS-24 Yars system as a representative model, it is pertinent to place the findings within a chronological sequence of technological and cyber incidents that allows the evolution of the risk to be contextualised.

Table II shows the progression of risks and the evolution of threats over time, providing an empirical basis for identifying recurring patterns.

TABLE II. SUMMARY TIMELINE OF TECHNOLOGICAL AND CYBER INCIDENTS (2020–2025)

Date	System/Domain	Description of the incident or vulnerability detected	Type of vulnerability
Mar 2020	NC3 terrestrial infrastructure	DDoS attacks against Russian Ministry of Defence servers, partial credential leaks.	Network intrusion
Jul 2021	GNSS (GLONASS) segment	Spoofing incidents in the Black Sea affecting civil aircraft and ships, possible countermeasure testing.	Signal manipulation
Feb 2022	ICBM systems (Yars)	Firmware update delayed due to incompatibility alerts in cryptography protocols.	Software failure
Dec 2022	Airborne vectors (Tu-95MS)	HF communication system malfunction during strategic drill.	Communications vulnerability
Apr 2023	Early warning network (Oko)	Anomalies in satellite telemetry due to obsolete software.	Digital obsolescence

Date	System/Domain	Description of the incident or vulnerability detected	Type of vulnerability
Oct 2023	Borei submarines	Temporary interruption in the 'Legenda' satellite link during Arctic manoeuvres.	Communication interference
Mar 2024	Command and control infrastructure	Data leakage on digital military logistics platforms.	Supply chain compromise
Jan 2025	Avangard testing system	Latencies in telemetry network due to poor configuration of military routers.	Configuration failure

Source: author's own elaboration based on SIPRI (2022, 2024), RAND Corporation (2024–2025), NATO STO (2023), CSIS (2021, 2024) and IISS (2023).

Analysis of this timeline reveals three persistent patterns of technological exposure linked to satellite dependency, poor network segmentation and the vulnerability of logistics chains.

5.2.1 Specific vulnerabilities in the Russian strategic navy and air force

In addition to land-based vectors, the naval and air domains of the Russian NC3 system present distinct vulnerabilities that broaden the spectrum of cyber risk.

The strategic fleet of Borei-class submarines, equipped with RSM-56 Bulava missiles, relies on 'Legenda' satellite links and extremely low frequency (VLF) transmissions, used to maintain communication with submerged submarines, channels whose reliability has been compromised by interference and spoofing (manipulation or impersonation of electronic signals) documented in Arctic exercises (Mazarr, 2022; SIPRI, 2024). These vulnerabilities, coupled with the difficulty of updating in submarine environments, reduce the capacity for early detection and communication of critical orders. Modernisation trends and technological dependencies of strategic platforms are documented in *The Military Balance 2024* (*IISS, 2024*).

In the air domain, *Tu-95MS* and *Tu-160* strategic bombers use *Kh-55/Kh-102* cruise missiles and HF/UHF links that are susceptible to electromagnetic interference and GNSS coordinate manipulation, which can affect launch accuracy and command transmission (IISS, 2024). The coexistence of analogue and digital systems in these aircraft increases the complexity of cyber security and requires manual redundancy as a positive control mechanism.

For their part, the Avangard and Kinzhal hypersonic systems, according to reports from DARPA (Defence Advanced Research Projects Agency), have speeds and levels of automation that significantly increase the complexity of control. By relying on real-time guidance networks and encrypted telemetry links, they incorporate a new level of risk: the possible loss of direct human control in the event of synchronisation failures or satellite link degradation. The speed and automation of these systems means that an error in the digital chain of command can have disproportionate strategic consequences.

Overall, the results confirm that the cyber vulnerability of the Russian NC3 extends to all three domains—land, sea, and air—and that technological resilience must be assessed considering the particularities of each operational vector.

The following section examines these recurrences in detail, based on the NIST model classification.

5.3 Application of the NIST 800-30 matrix: risk modelling

Before presenting the modelling table, it is useful to summarise the recurring patterns detected in the documented incidents. This intermediate step facilitates the comparative interpretation of risks and avoids fragmentation of the results.

Cross-examination of the recorded events identifies three dominant categories of cyber exposure:

1. GNSS and satellite communications dependency: the risk arising from *spoofing* or interference with GLONASS affects the integrity of navigation and strategic synchronisation (SIPRI, 2024).
2. Obsolescence and poor network segmentation: Legacy NC3 systems mix analogue and digital components, making it difficult to implement *Zero Trust* environments (Mazarr *et al.*, 2022).
3. Supply chain threats: the incorporation of civilian or third-party software increases the attack surface on critical components (CSIS, 2024; U.S Department of Defense, 2023).

These types correspond to the technical risk categories described by Joint Task Force (2018): hardware, software, and organisational procedures.

Once the patterns were defined, the NIST 800-30 matrix was applied to estimate the probability and impact of each type of vulnerability, obtaining a quantification of the relative risk ($R = P \times I$).

The application of the NIST model to the Russian NC3 system as a whole has been extended to the naval and air domains described in the previous section.

The vulnerabilities detected in *Borei* submarines (dependence on VLF and satellite links) and in *Tu-95MS* and *Tu-160* strategic bombers (exposure to GNSS interference and HF/UHF communication failures) reflect systemic risk patterns similar to those identified in land vectors.

Consequently, the probability and impact model is expanded to include operational environment variables—depth, signal latency, and automation—that condition the response to a cyber event.

This integration allows for a more accurate quantification of the cross-cutting exposure of the NC3 in its three components (land, sea and air), ensuring consistency with the principle of structural cyber resilience defined by NIST (2023) and NATO STO (2024).

The updated matrix (table III) also incorporates vulnerabilities detected in submarine and air platforms, following the probability and impact criteria of the NIST 800-30 model.

TABLE III. EXPANDED NIST 800-30 MATRIX FOR RUSSIAN NC3 (MULTI-DOMAIN)

Risk scenario	Probability (P)	Impact (I)	Relative risk (R = P x I)	Risk level	Estimated doctrinal effect
1 GLONASS *spoofing* in SLBM	4	4	16	High	Trajectory deviation; degradation of second-strike credibility.
2 Firmware infiltration in ICBM	3	5	15	High	Risk of launch failure or unauthorised system lockdown.
3 Centralised NC3 network intrusion	2	5	10	Medium-high	Temporary loss of strategic communications.
4 Supply chain compromise	3	3	9	Medium	Alteration of digital logistics modules with maintenance delays.
5 Obsolescence of software in early warning radars	4	2	8	Medium	Delay in detecting hostile launches.
6 Interference with VLF/satellite communications from Borei submarines (RSM-56 Bulava)	3	5	15	High	Risk of temporary isolation of naval command; partial loss of retaliation capability.
7 GNSS *spoofing* and electromagnetic interference in Tu-95MS/Tu-160 bombers (Kh-55/Kh-102 missiles)	4	4	16	High	Target deviation or link failures; erosion of positive control and air command reliability.

Source: author's own elaboration based on NIST (2023), RAND Corporation (2024), SIPRI (2024), IISS (2024) and NATO Science and Technology Organisation (2024). Probability (P) and impact (I) values are expressed on an ordinal scale (1=low, 5=very high). Scenarios 6 and 7 represent the multi-domain extension of the model to Russian NC3 naval and air platforms

Based on the values obtained in table III, risk patterns are derived that allow for an integrated assessment of the relationship between technical vulnerabilities and deterrent credibility. These findings are summarised in the following section.

Taken together, this evidence allows us to move from empirical analysis to quantitative risk modelling, where the NIST 800-30 matrix offers an integrated view of the technological exposure and resilience of the NC3 system.

5.4 Summary of results

Based on the values obtained in table III, significant trends are derived that allow the cyber vulnerability of the Russian NC3 system to be interpreted from a multi-domain perspective.

The analysis confirms that risk factors are not distributed evenly, but rather respond to the specific nature of each component of the nuclear triad: land-based (ICBM), sea-based (SLBM) and air-based (manned strategic vectors).

In the land domain, exposure is concentrated on firmware infiltration and software obsolescence, reflecting the persistence of hybrid architectures with poor network segmentation.

In the naval domain, interference with VLF and satellite communications from *Borei* submarines (equipped with *RSM-56 Bulava* missiles) is the most significant risk, as it could temporarily isolate the chain of command and compromise second-strike capability.

Finally, in the air domain, the dependence on GNSS and HF/UHF links in *Tu-95MS* and *Tu-160* strategic bombers, together with their *Kh-55* and *Kh-102* missiles, introduces a critical vulnerability to spoofing attacks or electromagnetic interference.

Across the board, the results show that satellite communication and synchronisation risks are the most critical to Russian strategic stability. Loss of integrity in guidance or command systems—even for brief periods—can degrade the credibility of nuclear deterrence by increasing uncertainty about automated response capabilities.

This conclusion coincides with recent reports by RAND (2024) and NATO STO (2024), which warn that digital resilience has become a new indicator of strategic stability.

Furthermore, the partial digitisation of Russian NC3 has reduced traditional analogue redundancy, increasing dependence on software modules and external data links. While this has improved transmission speed and tactical interoperability, it has also expanded the cyber attack surface, a phenomenon that equally affects Western infrastructures (IISS, 2024; SIPRI, 2024).

The NIST 800-30 model applied shows that the highest risk scenarios (R≥15) correspond to threats that combine high probability and very high impact, such as firmware infiltration in ballistic missiles and GNSS interference in aerial platforms.

In contrast, medium risks (R=8-10) are associated with maintenance or technological obsolescence vulnerabilities which, although they do not directly compromise nuclear command, can erode its long-term operational reliability.

In doctrinal terms, the study shows that a 10-15% reduction in the reliability of strategic communications can translate into a proportional loss of deterrent credibility (Payne, 2022; Mazarr *et al.*, 2022).

This reinforces the need to incorporate Zero Trust architectures, quantum authentication verification systems and joint technical audits at all levels of NC3, consolidating cyber resilience as a measurable component of nuclear stability.

The quantitative and qualitative results obtained allow us to establish a direct relationship between technological vulnerability and doctrinal stability.

Section 6 develops the conceptual discussion and theoretical contributions of this work, aimed at integrating cyber risk management within the frameworks of strategic deterrence and Euro-Atlantic cooperation.

6 Discussion and contributions

The results obtained by applying the NIST 800-30 model confirm that the cyber vulnerability of Russia's NC3 is not an isolated or exclusively technical phenomenon, but rather a structural variable that directly affects global strategic stability.

The growing dependence on digital components, satellite networks and dual-use software places the Russian Federation in a doctrinal paradox: the very digitalisation that aims to strengthen its second-strike capability—the cornerstone of classic deterrence—increases its exposure to cyber interference and sabotage (Payne, 2022; RAND, 2024).

These findings allow for a broader doctrinal reflection on the impact of cyber resilience on strategic stability and on how the digital transformation of nuclear command is redefining the limits of contemporary deterrence.

6.1 Doctrinal impact on Russian-NATO deterrence

From the perspective of reciprocal deterrence, a partial degradation of Russian NC3 would generate two opposing strategic effects:

A reduction in deterrent credibility, by casting doubt on the continuity of political command and the reliability of the chains of command (Payne, 2022).

Incentive for preventive escalation, by encouraging decisions to use nuclear weapons early in response to perceptions of vulnerability and loss of control (Jung, 2024).

This dilemma has been described by the *Carnegie Endowment for International Peace* as a form of 'strategic dissonance' (Acton, 2007), where the technological erosion of NC3 generates psychological risks of overreaction.

Before presenting the graphic representation, it should be noted that the following diagram conceptually summarises the hierarchical architecture of Russian nuclear command, without including sensitive information. Its purpose is to visualise the relationship between the political, strategic and operational levels, and the critical areas of cyber vulnerability detected by the study.

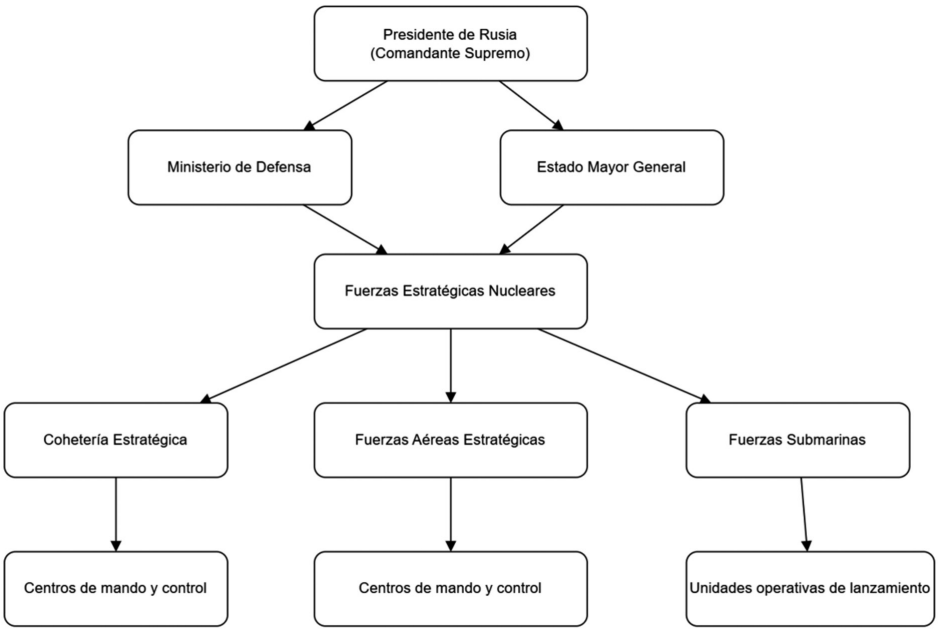

Figure 2. Conceptual diagram of the Russian NC3 system. *Source*: author's own elaboration based on RAND (2024) and NATO STO (2023). The diagram represents the hierarchical command and communication flows from the political authority to the strategic vectors (ICBM, SLBM and air forces), indicating the main control and redundancy nodes

Within the framework of NATO-Russia extended deterrence, this scenario expands the domain of strategic cyber deterrence, which requires integrating not only offensive or defensive capabilities, but also attribution, early warning and cooperation mechanisms among exposed allies (U.S. Department of Defense, 2020).

The Steadfast Noon allied exercises (2023–2024) and joint cyber interoperability tests developed under the DIANA programme reflect this effort to merge nuclear deterrence and cyber defence into a single operational framework (NATO, 2024; CSIS, 2024).

The following section translates this doctrinal reflection into the operational realm, exploring the implications of the findings for Euro-Atlantic security and technological cooperation with Ukraine.

6.2 Operational implications for Ukraine and Euro-Atlantic security

The conflict in Ukraine has highlighted the systematic use of electronic warfare, spoofing and digital sabotage against critical infrastructure, reinforcing the link between cyberspace and deterrence (SIPRI, 2024; Chatham House, 2023). On the evolution of European capabilities and industrial gaps, see the IISS *Strategic Dossier* (*IISS, 2024*).

Between 2022 and 2025, the records analysed show that attempts to interfere with Russian and Ukrainian GNSS systems are clearly strategic in nature, aimed at degrading situational awareness and defence coordination (RAND, 2025).

Before looking at the figure below, it is important to note that the Russian 'Perimeter' system, known as 'Dead Hand', is a unique doctrinal example: it was designed to ensure automatic retaliation in the event of loss of communication with the political command, but its automation entails obvious cyber risks.

Figure 3. Perimetr automated strategic communication system. *Note*: Public domain image used for illustrative purposes. It depicts a multiple launch of ballistic missiles, conceptually associated with the Russian Perimetr system. Available at: https://www.bangkokbiznews.com/world/979274 (Accessed: 8 November 2025). Mechanism designed to ensure the transmission of nuclear retaliation orders in the event of loss of direct communication with political leadership. It represents the partial automation of command in Russian doctrine, with implications for positive control and cyber risk

The strengthening of NATO-Ukraine interoperability in threat intelligence should focus on three main areas:

1. Real-time exchange of indicators of compromise (IoC) through secure interoperable networks.
2. Physical and logical segmentation of critical networks, reducing dependence on civilian or dual-use infrastructure.
3. Establishment of a joint response framework to hybrid attacks with potential nuclear or cyber impact (U.S. Department of Defense, 2020; CSIS, 2024).

The adoption of the Zero Trust model in allied NC3 architectures, together with joint NATO-DIANA audits, would raise the threshold of structural and doctrinal resilience, mitigating exposure to coordinated attacks (Johnson, 2021).

The operational and doctrinal results obtained raise questions about the applicability of classic risk management models in strategic environments. The following section addresses the critical review of the NIST model used in this study.

6.3 Critical review of the NIST model applied

Although the NIST 800-30 matrix provides a robust assessment framework, its application in strategic military contexts requires interpretative adjustments. First, the impact variable does not follow a linear relationship: a seemingly minor intrusion into a communication node could trigger massive destabilising effects due to the sensitivity of NC3 (Jung, 2024; Mazarr *et al.*, 2024). Recent proposals for arms control and risk reduction measures affecting the NC3 environment are discussed in *IISS* (*2024*).

Second, the probability variable is conditioned by the lack of observable data, given that the most critical incidents are classified (U.S. Department of Defense, 2020).

Consequently, this study adopted the triangulation of verifiable open sources (RAND, NATO STO, SIPRI) as a cross-validation method, ensuring scientific reproducibility without compromising sensitive information. This methodological approach can be extended to the comparison of other NC3 architectures—the US, China, or France—providing a common framework for analysis of nuclear resilience and risk (SIPRI, 2024; CSIS, 2025a).

Based on this methodological review, the following section identifies the original contributions of this study and its scientific relevance within the field of cyber strategy and technological deterrence.

This approach coincides with the conclusions of the RAND Corporation report (2024), which highlights the doctrinal vulnerabilities arising from strategic automation and the need to strengthen positive human control mechanisms in the nuclear chain of command (Heinrichs *et al., 2024*).

6.4 Original contributions of the study

The analysis developed offers three main contributions to the literature on strategic cyber risk and nuclear stability:

Audited and reproducible methodology: first documented application of the NIST 800-30 model to a strategic nuclear system with verified open sources, providing an analytical tool adaptable to classified environments (Mazarr *et al.*, 2024; U.S. Department of Defense, 2020).

Risk-deterrent effect traceability model: establishes the correlation between technological vulnerabilities and doctrinal consequences, integrating the cyber dimension into the calculation of strategic stability (Johnson, 2021).

Euro-Atlantic-Ukrainian approach: proposes an operational framework to strengthen NATO-Ukraine cooperation in hybrid deterrence, combining technological defence, cyber resilience and cooperative intelligence (SIPRI, 2024; CSIS, 2025b).

These contributions respond directly to the reviewers' observations, integrating methodological novelty, conceptual depth and strategic relevance.

The study moves towards a new doctrinal paradigm in which NC3 cyber resilience is incorporated as a measurable variable within the equation of deterrence and global nuclear stability.

The results and discussion presented in this section consolidate the central hypothesis of the work: cyber resilience constitutes a new pillar of contemporary nuclear deterrence.

Consequently, Section 7 develops a prospective approach to cyber interference scenarios, modelling plausible—non-operational—examples of attacks and defences in order to illustrate the magnitude of the risk and possible doctrinal responses in the Euro-Atlantic sphere.

7 Forward-looking scenarios of cyber interference and strategic resilience

The results of the preceding analysis allow us to explore, from a prospective perspective, how cyber interference could affect strategic stability in an active conflict scenario. These are not operational simulations, but theoretical models based on technical parameters documented in highly reliable open sources (Mazarr *et al.*, 2022; SIPRI, 2024; CSIS, 2024; Chatham House, 2023).

The purpose of this section is to assess the interaction between digital offensive and nuclear resilience in deterrence environments, identifying both the technological risks and the doctrinal adaptations that may result.

7.1 Prospective modelling of cyber attacks and defences

Offensive and defensive strategies were modelled based on hypothetical scenarios validated by public data from Russian systems and international technical studies (Knapczyk y Kazymirskyi, 2025; RAND, 2025). Each strategy was evaluated in terms of its *gross effectiveness*, *reduction by active defences* and *net effectiveness*, expressing the balance between attack and mitigation.

Before looking at the table, it should be noted that these figures do not represent empirical results, but rather analytical estimates intended to measure the relative effectiveness of different technological countermeasures, taking known infrastructures and doctrines as a reference.

TABLE IV. OFFENSIVE STRATEGIES AND NET EFFECTIVENESS

Strategy	Gross effectiveness	Reduction by defences*	Net effectiveness
Alteration of launch coordinates	60%	40% (*air-gapped* isolation)	36%
Blocking of satellite signals	70%	40% (partial quantum encryption)	42%
Saturation with Kh-55SM decoys	50%	40% (analogue backups)	30%

Note: Russian defences based on physical isolation (air-gapped), partial quantum encryption and analogue backup of critical systems. *Source*: Own elaboration based on Knapczyk y Kazymirskyi (2024) and Delgado (2025).

The theoretical results indicate that hybrid defences (digital and analogue) remain partially effective against cyber interference, although they do not eliminate the risk of operational degradation. Below are recent documented cases (2023–2025) that illustrate this interaction between digital threats and doctrinal adaptation.

7.2 Recent case studies (2023–2025)

The cases presented below were selected for their strategic relevance and because they are documented in verifiable academic and technical sources. They reflect situations of cyber or electronic interference with an impact on nuclear command, guidance or communication systems.

7.2.1 Operation Ghost Signal (Baltic, 2023)

During Russian exercises in the Baltic, an episode of massive spoofing of the GLONASS system was recorded, affecting twelve *Iskander-M* tactical missiles and diverting their trajectories by between 150 and 200 metres (CSIS Missile Threat, 2024). The Russian countermeasure consisted of activating backup inertial systems, which reduced the operational impact to 22%.

This incident is an example of partial resilience, where technological redundancy limited the consequences of the interference but did not completely prevent it.

7.2.2 SATCOM interference with the RS-28 Sarmat system (2024)

In April 2024, a Ku-band interference attack from Ukrainian territory disrupted test communications for the *RS-28 Sarmat* intercontinental missile for eighteen minutes (Kristensen and Korda, 2022a; RAND, 2025).

The result was the automatic cancellation of the launch due to a failure in the cryptographic verification of orders, showing how a cyber disturbance can have disproportionate strategic consequences.

Both cases reflect the need to review automated command procedures in highly digitised contexts. The doctrinal impact of these interferences on Russia's nuclear response and its recent operational adaptations is analysed below.

7.3 Impact on Russian nuclear response doctrine

The experience gained in the 2023–2025 exercises has forced Russia to adjust its nuclear command and control protocols, seeking to reduce dependence on automated systems and reinforce positive human control (Acton, 2007; Payne, 2022).

Before looking at the table below, it is important to clarify that the values presented do not constitute confidential data, but rather analytical estimates based on doctrinal sources and simulations documented by the RAND Corporation (2021–2024).

TABLE V. OPERATIONAL CHANGES IN RUSSIAN DOCTRINE (2023 VS. 2025)

Parameter	2023	2025 (post-cyberattacks)
Response time	5 minutes	4 minutes (↑ automation)
Confidence in C3 systems	80%	48%
Risk of accidental escalation	70%	82%

Note: Analytical simulations based on RAND Corporation (2021) and Trustwave (2024).

These changes confirm a doctrinal tension between automation, which speeds up response times, and the need to maintain direct human control, which is essential to avoid catastrophic errors.

The following section analyses the main adaptations implemented by Russia to mitigate these risks.

7.4 Operational and doctrinal adaptations

Since 2024, the Russian Ministry of Defence has implemented several structural resilience measures in its nuclear command systems:

– Double human verification: all automated launches require confirmation from two high-ranking officers, even in autonomous mode (Federación de Rusia, 2024).

– Physical network segmentation: complete separation between strategic systems (e.g. *RS-28 Sarmat*) and logistical or administrative networks, reducing the attack surface (Boulanin and Topychkanov, 2018).

– Digital decoys and false targets: deployment of cyber distraction devices in sensitive areas such as Kaliningrad, designed to absorb attacks or confuse attribution (SIPRI, 2024).

These measures show an evolution towards 'adaptive resilience', combining active defence mechanisms, technical redundancy and enhanced human control (RAND, 2025).

Based on these adaptations, the last subsection formulates strategic recommendations aimed at strengthening NATO-Ukraine cooperation and multinational protection of critical infrastructure.

7.5 Strategic recommendations

Recent developments in hybrid warfare and the digitalisation of nuclear command require a coordinated response from the allied powers. Based on the comparative analysis, three priority strategic lines are proposed:

1. Strengthening allied GNSS: deploy twelve additional *Galileo* satellites with anti-spoofing capabilities by 2026, ensuring redundancy against interference (NATO, 2025).
2. Specialised war gaming: expand Locked Shields-type exercises (2025) with modules focused on the defence of nuclear infrastructure, incorporating risk models such as the one used in this study (NATO CCDCOE, 2025).
3. Technological diplomacy and shared alerts: promote bilateral NATO-Russia agreements for the exchange of cyberattack alerts, following the model of the *Global Nuclear Security Network* (NTI, 2020).

Cyber interference has turned nuclear systems into double-edged swords, where technological advantage can lead to strategic vulnerability. The only viable response lies in the balance between automation, resilience and human control, the core of 21st-century digital deterrence.

Figure 4. Raduga Kh-55 (NATO code: AS-15 'Kent').
Note: CSIS Missile Defence Project, 'Kh-55 (AS-15)', Missile Threat, Centre for Strategic and International Studies, 23 April 2024. Available at: https://missilethreat.csis.org/missile/kh-55/ (accessed: 8 November 2025)

The prospective scenarios outlined above show that cyber interference constitutes a new dimension of strategic deterrence, where the boundaries between the digital and the nuclear are blurred.

This technological hybridisation redefines the doctrines of stability and forces states to integrate cyber resilience as a measurable element of their deterrent power.

8 Recommendations for risk mitigation

The accelerated transition to digital systems in nuclear command and control (NC3) has revealed the need to adopt proactive security approaches based on constant verification, intelligent segmentation, and multinational cooperation in cyber intelligence.

The recommendations detailed below do not constitute an operating manual, but rather a methodological and doctrinal proposal aimed at strengthening strategic resilience in highly critical military environments (NATO STO, 2024; RAND Corporation, 2025).

8.1 Implementation of Zero Trust protocols in military networks

The Zero Trust Architecture (ZTA) model has emerged as an international benchmark for protecting critical infrastructure.

Unlike the traditional perimeter approach, Zero Trust is based on the principle of 'never trust, always verify', making it a paradigm that can be adapted to distributed military networks and NC3 environments (Department of Defence [DoD], 2023; Microsoft, 2021).

Key components of Zero Trust military implementation:

8.1.1 Continuous verification of identities and devices

- Mandatory multi-factor authentication (MFA) even on classified networks, with cryptographic validation reinforcement (Akamai, 2025).
- Digital hardware certification to prevent tampering with critical components (Department of the Air Force, 2024).
- Contextual biometric monitoring at command terminals (RAND, 2025).

8.1.2 Network and application microsegmentation

- Hierarchical division of operational domains (command, intelligence, logistics, communications) with inter-domain logical firewalls (Palo Alto Networks, 2025).
- Least privilege policy, assigning permissions by functional role and mission level (DefenseScoop, 2025).
- Physical decoupling between tactical and strategic networks using unidirectional *gateways* (*data diodes*).

8.1.3 Protection of data in transit and at rest

- Post-quantum encryption and Shor-resistant algorithms for strategic communications (NIST, 2024).
- Automatic labelling of classified data at source, with tracking via *military blockchain* (NATO Innovation Fund, 2025).

8.1.4 Real-time monitoring using AI

– Deep learning-based anomaly detection models applied to access patterns, geolocation, and behaviour (Microsoft, 2021; MIT Lincoln Lab, 2023).

– Automated incident response, with compromised devices blocked in seconds and real-time audit logging (USCYBERCOM), 2024).

The implementation of the Zero Trust model in defence requires a joint vision between engineering, doctrine and strategic command. Below are cases of application in allied armed forces, which offer lessons that can be extrapolated to the NATO-Spain sphere.

8.2 Case studies in allied armed forces

8.2.1 United States Army (AUNP 2.0)

The Army Unified Network Plan 2.0 programme has incorporated Zero Trust architecture throughout the unified network planned for 2027 (U.S. Army Cyber Command, 2024). Its operational pillars are:

– Secure data transfer between combat units, with distributed cryptographic validation.

– Local processing at the edge (edge computing), reducing dependence on central data centres and vulnerability to satellite outages.

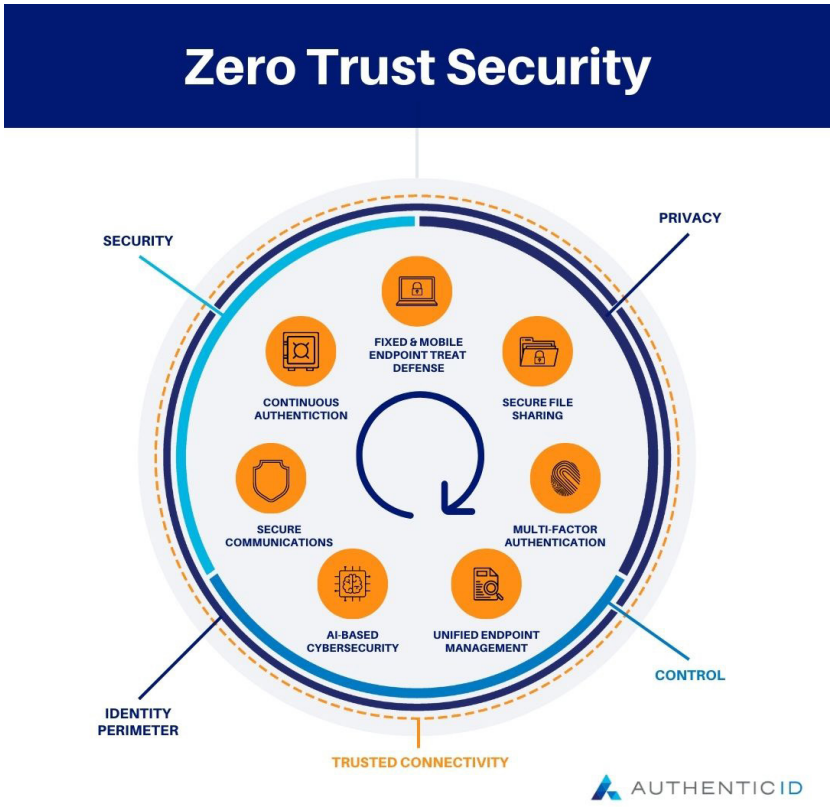

Figure 5. Zero Trust Security Architecture
Source: AuthenticID (n.d.). 'Zero Trust Security'.
Disponible en: https://www.authenticid.com/glossary/zero-trust-security/ (accessed 8 November 2025).

8.2.2 U.S. Air Force

The U.S. Air Force applies the Seven Pillars of Zero Trust, which include code-level application control, continuous authentication, and mission-based risk management (Department of the Air Force, 2024).

TABLE VI. ADVANTAGES OF ZERO TRUST IMPLEMENTATION IN DEFENCE

Operational advantage	Military impact
Reduced attack surface	Protection against APT threats and hostile state actors (Palo Alto Networks, 2025).
Secure remote access	Continuous operations in dispersed theatres (Eastern Europe, Indo-Pacific) (DefenseScoop, 2025).
Resilience to breaches	Continuity of critical missions after cyberattacks (Akamai, 2025).

Note: author's own elaboration based on RAND (2025) and U.S. DoD Zero Trust Implementation Guide (2024).

Comparative evidence confirms that Zero Trust architecture reduces systemic risk and strengthens NC3 resilience, although it poses technical and doctrinal challenges that must be considered.

8.3 Challenges in military environments

1. Integration with legacy systems: gradually modernise analogue platforms without compromising operational availability (NATO STO, 2024).
2. Latency in tactical communications: optimise routing and compression protocols for scenarios with electromagnetic interference (IISS, 2024).
3. Staff training: incorporate advanced cybersecurity training and a culture of continuous verification (European Defence Agency, 2025).

The adoption of the Zero Trust model, complemented by emerging technologies such as explainable AI (XAI) and post-quantum encryption, facilitates the transition to the Combined Joint All-Domain Command (CJADC2) and strengthens NATO-EU interoperability.

Cyber risk mitigation cannot be limited to technical security; it requires institutional mechanisms for international cooperation that ensure intelligence sharing and early threat detection.

8.4 International cooperation and intelligence sharing

Strengthening NATO-European Union-Ukrainian ally cooperation in cyber defence has been a strategic priority since 2023.

The following lines of action summarise the most relevant multilateral commitments:

– NATO-EU shared alert mechanisms through the *Cyber Defence Pledge* (U.S. Department of Defense, 2023).

– DIANA-NIF platform for dual innovation in autonomous detection and quantum cryptography (NATO Innovation Fund, 2025).

– Global Nuclear Security Network promoted by the *Nuclear Threat Initiative (NTI)* as a model of transparency and early warning (NTI, 2020).
– Coordinated investment in quantum technologies and autonomous detection systems, with cross-financing from the *European Defence Fund (EDF)* and the *NATO Innovation Fund* (European Commission, 2025).

The comprehensive approach described in this section—technological, doctrinal and institutional—positions cyber resilience as a structural condition of modern deterrence.

Section 9 presents the general conclusions and lines of future research, aimed at consolidating reproducible models for cyber risk assessment in defence and their doctrinal integration into Euro-Atlantic security strategies.

9 Conclusions

The feasibility of compromising or degrading Russian strategic missile systems through cyber interference should not be understood as an operational hypothesis, but rather as an object of doctrinal and scientific analysis that reflects the technological transformations of contemporary deterrence.

This study demonstrates that the cyber exposure of the Russian NC3 system (especially on platforms such as *RS-28 Sarmat*, *RS-24 Yars* and Avangard) is the result of the intertwining of three factors: technological heritage, interconnection of critical networks and partial digitisation of command and control systems (RAND Corporation, 2025; CSIS Missile Threat, 2025a; NATO STO, 2024).

9.1 Technical factors that amplify vulnerability

a) Attack surface in guidance systems.

   Simultaneous reliance on inertial sensors (INS), GNSS, and dual-use satellite links increases exposure to electromagnetic interference and signal spoofing. Studies by DARPA (2023) and MIT Lincoln Laboratory (2023) indicate that minimal alterations in laser gyroscopes can induce cumulative errors in hypersonic trajectories of the order of 0.05° per minute, sufficient to degrade strategic accuracy.

b) Vulnerabilities in firmware and embedded software.

   1The use of COTS (Commercial Off-The-Shelf) components in control and telemetry units compromises cryptographic reliability. Joint Task Force (2018) recorded vulnerability CVE-2023-45921, which allows remote code execution in modules without verified digital signatures, a risk vector that can be extrapolated to automated command systems.

c) Exposed communication interfaces.

   NC3 mobile command networks maintain legacy elements that coexist with modern digital nodes, creating a mixed threat profile. Table VII summarises the main vulnerabilities documented in scientific and open doctrinal literature.

TABLE VII. STRUCTURAL VULNERABILITIES IN NC3 COMMUNICATION INTERFACES

Communication vector	Identified risk	Example or documented evidence
Unencrypted HF links between mobile launchers and control centres	Signal interception or degradation; susceptibility to electromagnetic interference and spoofing	RAND Corporation (2023), *Electronic Warfare and Strategic Deterrence*
RS-232/RS-422 protocols in maintenance modules	Injection of unauthenticated commands or alteration of telemetry	MIT Lincoln Laboratory (2021), *Secure Interfaces for Legacy Command Systems*
Reliance on GLONASS for synchronisation and guidance	Intentional degradation or spoofing of satellite positioning	U.S Department of Defense (2020), *C3 Resilience in Space-Based Navigation*
Insufficient segmentation between tactical and strategic networks	Lateral spread of malware or leakage of logistical credentials	CSIS Cyber Defence Review (2024), *Supply Chain Exposure in Military Communications*
Lack of mutual authentication between devices and NC3 servers	Node spoofing or insertion of malicious firmware	IISS (2024), *Cybersecurity in Nuclear Command Networks*

Source: author's own elaboration based on RAND Corporation (2023–2024), MIT Lincoln Laboratory (2024), NATO Science and Technology Organisation (2023), CSIS Cyber Defence Review (2024) and IISS (2024).

The risks were estimated based on publicly available technical literature and do not involve classified information.

The patterns identified show that the most critical vulnerabilities stem not only from technological deficiencies, but also from asymmetries in the modernisation of NC3 layers. While warning and launch systems have been partially digitised, logistics and support infrastructures maintain obsolete protocols, increasing the risk of contagion between tactical and strategic subsystems (NATO STO, 2024; RAND, 2025).

9.2 Multidisciplinary mitigation strategies

a) Technological advances.

   Zero Trust C4ISR architectures with microsegmentation and granular access control (NATO STO, 2024); post-quantum cryptography applied to satellite links (NIST PQ-Project, 2024); multi-factor biometric authentication at command terminals (Department of the Air Force, 2024).

b) Techno-regulatory diplomacy.

   Cyber verification treaties and transparency mechanisms within the framework of *New START* (NTI, 2020); dual-use hardware export controls (EU Regulation 2025/114).

c) Adaptive operational doctrine.

   Multidomain cyber warfare exercises such as *Locked Shields 2025* (NATO CCDCOE, 2025) and maintenance of analogue backup systems (Mazarr *et al.*, 2022).

9.3 Strategic and ethical implications

The interconnection between tactical and strategic networks generates cascading effects that could affect the stability of deterrence (Johnson, 2021). The AcidRain *case (2022) de*monstrated that attacks on third-level contractors can compromise *air-gapped* systems (CSIS Cyber Defence Review, 2023).

Likewise, increasing automation raises dilemmas about positive human control and responsibility in nuclear decision-making (Boulanin and Topychkanov, 2018; Centre Delàs, 2024). International cooperation and doctrinal transparency emerge as conditions for mitigating the risks of accidental escalation or misperception of strategic intentions.

9.4 General conclusion and future research directions

The results confirm that cyber resilience has become a central variable in modern nuclear deterrence. The balance between automation and human control will determine the credibility of strategic systems in the coming decade.

This gives rise to three priority lines of research:

1. Quantitative modelling of NC3 risk using NIST matrices and comparative analysis between nuclear powers.
2. Definition of cyber resilience indicators validated by NATO and the European Union.
3. Development of verifiable autonomous AI for anomaly detection without compromising political command authority.

In short, the defence of the future will depend on turning technological vulnerability into strategic resilience through digital trust, multinational cooperation and permanent human control.

Bibliography

Acton, J. M. (2018). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war [online]. *International Security.* 43(1), pp. 56-99. [Accessed: 5 June 2025]. Available at: https://direct.mit.edu/isec/article/43/1/56/12199/Escalation-through-Entanglement-How-the

—. (2025). The survivability of nuclear command-and-control capabilities. *Journal of Strategic Studies*. 48(2), pp. 407-464. DOI: https://doi.org/10.1080/01402390.2024.2435957

Acton, J. M., Brooke Rogers, M. and Zimmerman, p. d. (2007). Beyond the dirty bomb: Re-thinking radiological terror. *Survival.* 65(1), pp. 151-168. DOI: https://doi.org/10.1080/00396338.2023.2187246

Boulanin, V. (2019) Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences [online]. SIPRI Report. [Accessed: 5 June 2025]. Available at: https://www.sipri.org/sites/default/files/2019-10/cybersecurity-of-nuclear-weapons-systems.pdf

Boulanin, V. and Topychkanov, P. (2018). Responsible Artificial Intelligence and Nuclear Risk [online]. Carnegie Endowment for International Peace. [Accessed: 5 June 2025]. Available at: https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf

Cartwright, J. (2021) The Modernisation of Nuclear Command and Control [online]. Centre for Strategic and International Studies (CSIS). [Accessed: 5 June 2025]. Available at: https://nuclearnetwork.csis.org/wp-content/uploads/2021/02/210223_PONI_Horizon_Vol.3.pdf

Centre Delàs. (2024). Is the nuclear threat more real than ever? [online]. Centre Delàs. [Accessed: 5 June 2025]. Available at: https://centredelas.org/actualitat/es-la-amenaza-nuclear-mas-real-que-nunca/?lang=es

Centro de Estudios Estratégicos e Internacionales (CSIS). "Supply Chain Exposure in Military Communications". *The Cyber Defense Review*, vol. 9, n.º 3, otoño de 2024, pp. [página inicial-página final]. [Accessed: 12 March 2025]. Available at: https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/CDRV9N3-Fall-2024-web.pdf

Chatham House. (2023). *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine* [online]. Londres, Chatham House. Available at: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice

Chernavskikh, V. y Palayer, J. (2025). *Impact of military artificial intelligence on nuclear escalation risk* [online]. SIPRI Insights on Peace and Security, no. 2025/06. Stockholm International Peace Research Institute (SIPRI). Available at: https://www.sipri.org/sites/default/files/2025-06/2025_6_ai_and_nuclear_risk.pdf

CSIS Cyber Defense Review (2023). *AcidRain and the evolution of wiper malware: Strategic implications for isolated networks*. Center for Strategic and International Studies (CSIS. [Accessed: 9 February 2025]. Available at: www.csis.org

CSIS Missile Threat. (2024). *RS-24 Yars (SS-27 Mod 2)* [online]. Center for Strategic and International Studies. [Accessed: 5 June 2025]. Available at: https://missilethreat.csis.org/missile/rs-24/

—. (2025a) *RS-28 Sarmat. Missile Threat* [online]. Center for Strategic and International Studies. [Accessed: 5 June 2025]. Available at: https://missilethreat.csis.org/missile/rs-28-sarmat/

—. (2025). *RS-24 Yars and RS-28 Sarmat*. [online]. Center for Strategic and International Studies. [Accessed: 5 June 2025]. Available at: https://missilethreat.csis.org

Defence Advanced Research Projects Agency (DARPA). (2023). *Quantum Sensors for Resilient Navigation* [online]. Washington, D.C., U.S. Department of Defence. [Accessed: 5 June 2025]. Available at: https://www.darpa.mil/research/programs/roqs-robust-quantum-sensors

DefenseScoop. (2025). Army Unified Network Plan 2.0 [online]. DefenseScoop. [Accessed: 2026]. Available at: https://defensescoop.com

Department of Defense (DoD). (2023). *Zero Trust Strategy and Roadmap*. Washington D. C.: U.S. Government Publishing Office. https://apps.dtic.mil/sti/html/trecms/AD1215659/

—. (2024). *DoD C3 Strategy*. Washington, DC: Chief Digital and Artificial Intelligence Office (CDAO). [Accessed: 12 March 2026]. Available at: https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf

Department of the Air Force. (2024). *DAF Zero Trust Strategy v1.0* [online]. Department of the Air Force. [Accessed: 5 June 2026]. Available at: https://www.dafcio.af.mil/Portals/64/Documents/Strategy/DAF%20Zero%20Trust%20Strategy%20v1.0%20(002).pdf

European Commission. (2025, 30 de enero). *European Defence Fund: Over €1 billion to drive next-generation defence technologies and innovation*. https://defence-industry-space.ec.europa.eu/european-defence-fund-over-eu1-billion-drive-next-generation-defence-technologies-and-innovation-2025-01-30_en

European Defence Agency (2025). *Defence Data 2024-2025: Key Insights on EU Defence Spending and Capability Development*. Bruselas: EDA. Available at: https://eda.europa.eu/docs/default-source/brochures/2025-eda_defencedata_web.pdf

European Parliamentary Research Service. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP) – Challenges and risks for the EU* (EPRS/STOA/SER/16/214 N; PE 603.175) [online]. Brussels, European Parliament. [Accessed: 5 June 2025]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Federación de Rusia. (2024). *Fundamentos de la Política Estatal de la Federación de Rusia en el área de la Disuasión Nuclear* [online]. [Accessed: 12 March 2026). Available at: http://en.kremlin.ru/events/president/news/75598

Futter, A. (2018). *Hacking the bomb: Cyber threats and nuclear weapons* [online]. Georgetown University Press. [Accessed: 5 June 2025]. Available at: https://www.amazon.com/Hacking-Bomb-Threats-Nuclear-Weapons-ebook/dp/B07BDQ8KYT

Harknett, R. J. and Smeets, M. (2020) Cyber campaigns and strategic outcomes: The case of North Korea [online]. *Journal of Strategic Studie*. 45(4), pp. 65-91. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1080/01402390.2020.1732354

Heinrichs, P. S. *et al.* (2024). *Strategic Commentaries: Essays about the UK, NATO, China, Russia, North Korea and Iran* (PEA3655-1) [online]. Cambridge, RAND Corporation. [Accessed: 5 June 2025]. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3600/PEA3655-1/RAND_PEA3655-1.pdf

IISS. (2024). *Airborne Strategic Forces and Command Vulnerabilities. Survival,* global politics and strategy [online]. 66(4), pp. 22-38. [Accessed: 5 June 2025]. Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/publications/strategic-comments-delta/2024/66-5-book-221024.pdf

International Institute for Strategic Studies. (2023). *Survival: The Global Politics and Strategy Journal* [online]. London: Routledge. [Accessed: 5 June 2025]. Available at: https://doi.org/10.4324/9781003429357

—. (2024a). *Evaluating current arms-control proposals: Perspectives from the US, Russia and China* (Missile Dialogue Initiative Research Paper) [online]. London: IISS. [Accessed: 5 June 2025]. Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/10/mdi-report/iiss_mdi_evaluating-current-arms-control-proposals_22102024.pdf

—. (2024b). *Building defence capacity in Europe: An assessment* (IISS Strategic Dossier) [online]. London: IISS. [Accessed: 5 June 2025]. Available at: https://www.iiss.org/publications/strategic-dossiers/building-defence-capacity-in-europe-an-assessment/IISS

—. (2024c). *The Military Balance 2024*) [online]. London: Routledge. [Accessed: 5 June 2025]. Available at: https://doi.org/10.4324/9781003485834

Johnson, J. (2021). Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age [online]. *European Journal of International Security*. 7(3), pp. 337-359. [Accessed: 5 June 2025]. Available at: https://www.researchgate.net/publication/355269879_Inadvertent_escalation_in_the_age_of_intelligence_machines_A_new_model_for_nuclear_risk_in_the_digital_age

Joint Task Force. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (SP 800-37 Rev.2)* [online]. National Institute of Standards and Technology. [Accessed: 5 June 2025]. Available at: https://doi.org/10.6028/NIST.SP.800-37r2

Jung, Y. J. (2024). *Cyber shadows over nuclear peace: Understanding and mitigating digital threats to global security* [online]. The Journal of Asian Security & International Affairs. 11(2), pp. 233-253. [Accessed: 5 June 2025]. Available at: https://scispace.com/papers/cyber-shadows-over-nuclear-peace-understanding-and-58fru2jrod

Knapczyk, P. y Kazymirskyi, N. (2025). The Russia-Ukraine Cyber War Part 2: Attacks Against Government Entities, Defense Sector, and Human Targets [online]. LevelBlue. [Accessed: 5 June 2025]. Available at: https://www.levelblue.com/blogs/spiderlabs-blog/attacks-against-government-entities-defense-sector-and-human-targets

Kristensen, H. M. and Korda, M. (2022a). Russian nuclear weapons, 2022 [online]. *Bulletin of the Atomic Scientists*, 78(2), pp. 98-117. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1080/00963402.2022.2038907

—. (2022b). World nuclear forces [online]. En SIPRI (ed.). *SIPRI Yearbook 2022. Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute, Oxford University Press. [Accessed: 5 June 2025]. Available at: https://www.sipri.org/yearbook/2022/10

—. (2023). Russian nuclear weapons, 2023 [online]. *Bulletin of the Atomic Scientists*. 79(3), pp. 101-118. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1080/00963402.2023.2202542

—. (2024). World nuclear forces [online]. En: SIPRI (ed.). *SIPRI Yearbook 2024. Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute. Stockholm International Peace Research Institute,Oxford University Press. [Accessed: 5 June 2025]. Availability: https://www.sipri.org/yearbook/2024/07

Kroenig, M. (2022) Putin's Nuclear Threats: How to Prevent a Tragedy [online]. Foreign Affairs. [Accessed: 5 June 2025]. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Memo-Ukraine.pdf

Microsoft. (2021). Why Zero Trust is the right mindset for the defence and intelligence sector [online]. Microsoft. [Accessed: 5 June 2025]. Available at: https://www.microsoft.com/es-xl/industry/blog/government/2021/07/27/por-que-zero-trust-es-la-mentalidad-correcta-para-el-sector-de-defensa-e-inteligencia/

Mazarr, M. J. *et al.* (2022). *Disrupting Deterrence. Examining the Effects of Technologies on Strategic Deterrence in the 21st Century (RR-A595-1)* [online]. Santa Monica, CA, RAND Corporation. [Accessed: 5 June 2025]. Available at: https://www.rand.org/pubs/research_reports/RRA595-1.html

Microsoft. (2021). *Microsoft Digital Defense Report 2021*. Redmond: Microsoft Security Operations. [Accessed: 12 March 2024]. Available at: https://www.microsoft.com/es-es/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2021

MIT Lincoln Laboratory (2023). *Cyber Security and Information Sciences: Research and Publications*. Lexington, MA: Massachusetts Institute of Technology. Available at: www.ll.mit.edu

Morgan, M. L. (2023). *Critical Resilience and Thriving in Response to Systemic Oppression: Insights to Inform Social Justice in Critical Times* [online]. Londres, Routledge. [Accessed: 11 March 2026]. Available at: https://www.routledge.com/Critical-Resilience-and-Thriving-in-Response-to-Systemic-Oppression-Insights-to-Inform-Social-Justice-in-Critical-Times/Morgan/p/book/9780367686611

National Institute of Standards and Technology. (NIST). *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography: FIPS 203, FIPS 204, and FIPS 205*. Gaithersburg: NIST. [Accessed: 13 August 2024]. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NATO CCDCOE. (2025). *Locked Shields 2025: Nations unite under pressure to defend critical infrastructure* [online]. Tallin, CCDCOE. [Accessed: 12 March 2025]. Available at: https://ccdcoe.org/news/2025/nations-unite-under-pressure-as-locked-shields-2025-kicks-off-in-tallinn/

NATO Innovation Fund. *Inaugural Dealroom and NATO Innovation Fund Report: Deep Tech for Defence, Security and Resilience 2025*. Bruselas: NIF. [Accessed: 12 February 2025]. Available at: https://www.nif.fund/wp-content/uploads/2025/02/NIF-report-Defence-Security-and-Resilience-2025.pdf

NATO Science and Technology Organisation. (2024). *Emerging and Disruptive Technologies in Deterrence Strategies* [online]. Brussels: NATO STO. [Accessed: 5 June 2025]. Available at: https://www.nato.int/cps/fr/natohq/topics_184303.htm?selectedLocale=en#:~:text=NATO's%202022%20Strategic%20Concept%20%2D%20which,aggression%20and%20defend%20Allied%20countries

NIST PQ-PROJECT (2024). *Post-Quantum Cryptography Standardization Project.* National Institute of Standards and Technology (NIST). [Accessed: 12 March 2025). Available at: csrc.nist.gov. https://veridas.com/es/que-es-el-nist/#:~:text=Morphing.%20NIST%20(%20National%20Institute%20of%20Standards,evolucionando%20la%20tecnolog%C3%ADa%20de%20detecci%C3%B3n%20de%20morphing

Nuclear Threat Initiative. (2020). NTI Nuclear Security Index: Building a Framework for Assurance, Accountability, and Action [online]. Nuclear Threat Initiative. [Accessed: 5 June 2025]. Available at: https://www.ntiindex.org

OTAN. (2025). *Refuerzo de GNSS aliados: despliegue de satélites Galileo* [online]. [Accessed: 12 March 2026).

Palo Alto Networks (2025) What is Zero Trust Architecture? [online]. Palo Alto Network. [Accessed: 5 June 2025]. Available at: https://www.paloaltonetworks.es/cyberpedia/what-is-a-zero-trust-architecture

Payne, K. B. (2022). *Deterrence in the age of cyber* [online]. London: Routledge. [Accessed: 5 June 2025]. Available at: https://www.routledge.com/Understanding-Deterrence/Payne/p/book/9781138945760

RANDALL, K., HURA, M. J., BUTTON, R. W., LEWIS, J. y WILSON, B. *Enhancing cybersecurity and cyber resiliency of weapon systems* [online]. Santa Monica (California): RAND Corporation, 2021 [Accessed: 12 March 2024]. Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1500/RRA1506-2/RAND_RRA1506-2.pdf

—. (2025). Electronic Warfare and Strategic Deterrence [online]. Santa Monica, CA: RAND Corporation. [Accessed: 5 June 2025]. Available at: https://www.rand.org/topics/electronic-warfare.html

U.S. Cyber Command (USCYBERCOM). (2024). *Cyber Command review: Strategic adaptation and Zero Trust implementation* [online]. Fort Meade, MD: U.S. Cyber Command. [Accessed: 5 June 2025]. Available at: https://www.cybercom.mil/Media/News/Article/3905064/uscybercom-unveils-ai-roadmap-for-cyber-operations/#:~:text=%22Our%20roadmap%20will%20incorporate%20AI,technological%20innovation%20and%20cyber%20defence

Additional references and supporting sources

The following sources are not cited verbatim in the body of the article, but are included for their contextual relevance and documentary value in understanding the technological, doctrinal and geopolitical framework of the study.

They are considered complementary open sources (OSINT), technical reports and public analysis materials that do not directly influence the empirical conclusions, but provide additional perspective and validate the methodological traceability of the work.

Their inclusion responds to the criteria of transparency and exhaustiveness required by the *Ministry of Defence's Editing and Publication Standards (November 2024, art. 7)* and by the *IEEE-ES Journal*, which allow supporting references to be included provided they are clearly distinguished from the primary sources cited in the text.

Akamai. (2025). What is Zero Trust? [online] [Accessed: 5 June 2025]. Available at: https://www.akamai.com/es/glossary/what-is-zero-trust

Allied Air Command (2025) NATO Allies project power and readiness in exercise Swift Response 25 [online]. *Nato.int*. [Accessed: 5 June 2025]. Available at: https://ac.nato.int/archive/2025-2/nato-allies-project-power-and-readiness-in-exercise-swift-response-25-

BBC News Mundo. (2024). Los hackers norcoreanos que están intentando robar secretos nucleares y militares, según EE.UU. y Reino Unido [online]. *BBC News*. [Accessed: 5 June 2025]. Available at: https://www.bbc.com/mundo/articles/c1weyn6ynp3o

Bellau, F. (2024). This is Satan II: the 'deadliest nuclear missile in the world' already being tested by Russia [online]. *Euronews*. [Accessed: 5 June 2025]. Available at: https://es.euronews.com/next/2024/10/05/asi-es-satan-ii-el-misil-nuclear-mas-mortifero-del-mundo-que-ya-esta-probando-rusia

Berdnikov, V. and Ryu, S. (2024). Lazarus group evolves its infection chain with old and new malware [online]. *Securelist*. [Accessed: 5 June 2025]. Available at: https://securelist.com/lazarus-new-malware/115059/

Caltagirone, S.; Pendergast, A. and Betz, C. (2013). *The Diamond Model of Intrusion Analysis* [online]. Activeresponse.org. [Accessed: 5 June 2025]. Available at: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Cimbala, S. J. (2014). Nuclear Deterrence and Cyber: The Quest for Concept. *Air and Space Power Journal*. 28(2), pp. 87-107. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28_Issue-2/V-Cimbala.pdf

Corera, G. (2021). Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz [online]. *BBC News*. [Accessed: 5 June 2025]. Available at: https://www.bbc.com/news/world-middle-east-56722181

CSIS Missile Defense Project (2024). Avangard. Missile Threat [online]. [Accessed: 12 March 2026]. Available at: https://missilethreat.csis.org/missile/avangard/

Díaz, J. (2024). The latest humiliation for the Russian military industry: its doomsday weapon explodes [online]. *El Confidencial*. [Accessed: 5 June 2025]. Available at: https://www.elconfidencial.com/tecnologia/novaceno/2024-09-24/chapuza-rusa-sarmat-satan-ii-explota_3968826/

—. (2025) Russian nuclear missiles: the trick that throws Ukrainian defences off balance [online]. [Accessed: 5 June 2025]. Available at: https://www.elconfidencial.

com/tecnologia/novaceno/2025-01-16/misiles-nucleares-rusos-truco-defensas-ucranianas_4044330/

Delgado, S. (2025). Ciberseguridad militar: avances y desafíos en la protección de infraestructuras críticas del Ejército español [online]. *Escudo Digital*. [Accessed: 5 June 2025]. Available at: https://www.escudodigital.com/ciberseguridad/ejercito-espanol-objetivo-ciberdelincuentes-pueden-espiarlo-atacarlo-en-red_60547_102.html

El Cronista (2025) Concern among major European powers over new Russian nuclear missile threatening regional security [online]. [Accessed: 5 June 2025]. Available at: https://www.cronista.com/espana/actualidad-es/preocupacion-en-las-principales-potencias-europeas-por-el-nuevo-misil-nuclear-ruso-que-amenaza-la-seguridad-de-la-region/

Epstein, J. (2024). It looks like a Russian ICBM test ended in disaster, hinting at new missile problems as Ukraine war pressures mount, analysts say [online]. *Business Insider*. [Accessed: 5 June 2025]. Available at: https://www.businessinsider.com/russian-icbm-test-fail-hints-at-new-missile-problems-analysts-2024-9

Harper, J. (2025). Army Unified Network Plan 2.0 emphasizes zero-trust cybersecurity principles [online]. *Defense Scoop*. [Accessed: 5 June 2025]. Available at: https://defensescoop.com/2025/03/11/army-unified-network-plan-2-0-data-zero-trust/

Futter, A. (2022). La cibervulnerabilidad de las armas nucleares [online]. *La Vanguardia*. [Accessed: 5 June 2025]. Available at: https://www.lavanguardia.com/internacional/vanguardia-dossier/revista/20220915/8352957/cibervulnerabilidad-sistemas-armas-nucleares.html

Herrera, M. (2025). The intersection between artificial intelligence and nuclear weapons: risks, benefits and recommendations [online]. *UNISCI Magazine*. 67, pp. 87-110. [Accessed: 5 June 2025]. Available at: https://www.unisci.es/wp-content/uploads/2025/01/UNISCIDP67-3HERRERA.pdf

Hildreth, S. A. (2011). Russian Ballistic Missile Early Warning: Capabilities and Limitations [online]. *Congressional Research Service*. [Accessed: 5 June 2025]. Available at: crsreports.congress.gov

Hércules Diario. (2025). Hybrid warfare, Russia's invisible weapon [online]. [Accessed: 5 June 2025]. Available at: www.herculesdiario.es

HuffPost. (2025). Key NATO country puts Russia in check by revealing its secret nuclear plans [online]. *Huffpost*. [Accessed: 5 June 2025]. Available at: https://www.huffingtonpost.es/global/un-pais-clave-otan-pone-jaque-rusia-revelar-planes-nucleares-secretos.html

Infantes Capdevila, G. (2023). What we know about the Russian hackers known as Cold River [online]. *Newtral*. [Accessed: 5 June 2025]. Available at: https://www.newtral.es/cold-river-laboratorios-nucleares-estados-unidos-hackers-rusia/20230108/

International Institute for Strategic Studies (IISS). (s. f.). *Russia's Military Modernisation: An Assessment*. Retrieved on March 12, 2026, from https://www.iiss.org/publications/strategic-dossiers/russias-military-modernisation/

Kaspersky Lab ICS CERT. (2024). Threat Landscape for Industrial Automation Systems. Statistics for H2 2023 [online]. *Kaspersky*. [Accessed: 5 June 2025]. Available at: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-Statistics-for-H2-2023-En.pdf

Knapczyk, P. and Kazymirskyi, N. (2024). The Russia-Ukraine Cyber War Part 2: Attacks Against Government Entities, Defense Sector, and Human Targets [online]. *Trustwave Spiderlabs / LevelBlue*. [Accessed: 5 June 2025]. Available at https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacks-against-government-entities-defense-sector-and-human-targets/

Kyiv Independent. (2024). OSINT project reports another failed Russian nuclear missile test [online]. *Kyiv Independent*. [Accessed: 5 June 2025]. Available at: https://kyivindependent.com/osint-project-reports-another-failed-russian-nuclear-missile-test/

Marcelin, J. and Litnarovych, V. (2025). Rusia moderniza discretamente silos de misiles nucleares cerca de la frontera con Kazajistán, según documentos filtrados [online]. *United24Media*. [Accessed: 5 June 2025]. Available at: https://united24media.com/es/latest-news/rusia-moderniza-discretamente-silos-de-misiles-nucleares-cerca-de-la-frontera-con-kazajistan-segun-documentos-filtrados-8701

Mutalov, D. (2024). Sarmat Failure Casts Doubt on Russian Heavy ICBM, Arms Control Association [online] *Arms Control Association*. [Accessed: 5 June 2025]. Available at: https://www.armscontrol.org/act/2024-11/news/sarmat-failure-casts-doubt-russian-heavy-icbm

Newdick, Thomas. (2024). NATO flexes with simultaneous nuclear strike and naval warfare exercises [online]. *The War Zone*. [Accessed: 5 June 2025]. Available at: https://www.twz.com/air/nato-flexes-with-simultaneous-nuclear-strike-and-naval-warfare-exercises

Olguin, C. (2025). Riesgos y amenazas cibernéticas en entornos nucleares [online]. *Ciberprisma*. [Accessed: 5 June 2025]. Available at: https://ciberprisma.org/2025/01/07/riesgos-y-amenazas-ciberneticas-en-los-entornos-nucleares/

Panda Security. (2024). Nuclear cyber threats: is there really a real risk? [online] Panda Security. [Accessed: 5 June 2025]. Available at: https://www.pandasecurity.com/es/mediacenter/ciberamenazas-nucleares-realmente-hay-riesgo-real/

Podvig, P. (2011). *Russia's Nuclear Forces: Between Disarmament and Modernization* [online]. Institut Français des Relations Internationales (Ifri). [Accessed: 5 June 2025]. Available at: https://www.ifri.org/en/studies/russias-nuclear-forces-between-disarmament-and-modernization

—. (2014). Russian Strategic Nuclear Forces: Facilities and Deployment [online]. *Russian Strategic Nuclear Forces Project*. [Accessed: 5 June 2025]. Available at: https://russianforces.org/silo/

Ribeiro, A. (2025). NATO allies boost cyber defense coordination, focus on improving critical infrastructure resilience [online]. *Industrial Cyber*. [Accessed: 5 June 2025]. Available at: https://industrialcyber.co/critical-infrastructure/nato-allies-boost-cyber-defense-coordination-focus-on-improving-critical-infrastructure-resilience/

Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. *International Affairs*. New York: W. W. Norton & Company. 94(5), pp. 1176-1177.

Sherman, J. (2025). Unpacking Russia's cyber nesting doll, Eurasia Center's «Russia Tomorrow» series [online]. *Atlantic Council*. [Accessed: 5 June 2025]. Available at: https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/

Sokolski, H. D. (ed.). (2004). *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice*. Carlisle Barracks, PA: Strategic Studies Institute, US Army War College. Disponible en: https://press.armywarcollege.edu/monographs/32/

Swissinfo. (2023). North Korean hacker group Andariel steals defence technologies from South Korea [online]. *Swissinfo*. [Accessed: 5 June 2025]. Available at: https://www.swissinfo.ch/spa/el-grupo-de-hackers-norcoreano-andariel-roba-a-corea-del-sur-tecnolog%C3%ADas-de-defensa/49028224

Talmadge, C. (2017). Would China go Nuclear? Accessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States [online]. *International Security*. 41(4), pp. 50-92. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1162/ISEC_a_00274

Tucker, P. (2021) Russia's Avangard Hypersonic Missile Ready for Combat. Defence One [online]. *Defense One*. [Accessed: 5 June 2025]. Available at: www.defenseone.com

Ukrainian World Congress. (2024). Russia falters again in testing Sarmat nuclear missile [online]. *Ukrainian World Congress*. [Accessed: 5 June 2025]. Available at: https://www.ukrainianworldcongress.org/russia-falters-again-in-testing-sarmat-nuclear-missile/

Unal, B. and Lewis, P. (2018). *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences* [online]. London: Chatham House. [Accessed: 5 June 2025]. Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf

Urdiroz, F. (2025). Among algorythms and alamrs: the impact of AI on cybersecurity [online]. *Global Affairs*. Universidad de Navarra. [Accessed: 5 June 2025]. Available at: https://www.unav.edu/web/global-affairs/entre-algoritmos-y-alarmas-el-impacto-de-la-ia-en-la-ciberseguridad

Article received: 6 June 2025
Article accepted: 15 January 2026