Revista del Instituto Español de Estudios Estratégicos
ISSN-e: 2255-3479

Juan de Dios Meseguer González
Doctorando en Seguridad internacional en IUGM-UNED

Correo: jmeseguer1@alumno.uned.es

Análisis de los riesgos cibernéticos y la resiliencia en la tríada nuclear rusa

Analysis of Cyber Risks and Resilience in the Russian Nuclear Triad

Resumen

Este trabajo estudia la exposición tecnológica y la capacidad de resistencia del sistema de mando, control y comunicaciones nucleares (NC3) de Rusia, en el contexto de la competencia estratégica global y los desafíos emergentes de seguridad en el espacio euroatlántico. Se propone un modelo metodológico reproducible que combina revisión sistemática, análisis conceptual de arquitecturas de mando y control y simulación de escenarios basados en los estándares NIST 800-30 e ISO/IEC 27005.

La investigación utiliza inteligencia científica abierta y validada (OSINT) procedente de fuentes institucionales como RAND, NATO STO y SIPRI, transformando la ausencia de datos clasificados en una oportunidad para establecer una base analítica verificable. Desde una perspectiva interdisciplinar, se plantean marcos de mitigación y medidas de mejora fundamentadas en arquitecturas Zero Trust, procesos de auditoría de ciberresiliencia y mecanismos de verificación cruzada de información estratégica.

El estudio proporciona un esquema de referencia para comprender y evaluar los efectos de la digitalización militar sobre la estabilidad

estratégica contemporánea, ofreciendo un instrumento útil para investigadores y responsables de defensa interesados en el fortalecimiento de la seguridad tecnológica internacional.

Palabras clave

Seguridad estratégica, Ciberdefensa, Sistemas de mando y control, Disuasión tecnológica, Cooperación euroatlántica.

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 stability, Cyber-defense, Command and control systems, Technological deterrence, Euro-Atlantic cooperation.

Citar este artículo:

Meseguer González, J. D. (2025). Análisis de los riesgos cibernéticos y la resiliencia en la tríada nuclear rusa. *Revista del Instituto Español de Estudios Estratégicos*. 26, pp. 13-52.

1 Introducción

El riesgo cibernético en los sistemas estratégicos de mando, control y comunicaciones nucleares (NC3) se ha convertido en un factor crítico para la estabilidad internacional. La digitalización progresiva de los vectores de lanzamiento, la automatización de los protocolos de alerta temprana y la integración de inteligencia artificial en los procesos de decisión estratégica han incrementado la superficie de exposición ante ciberataques o interferencias. En este contexto, la tríada nuclear rusa —conformada por misiles intercontinentales basados en tierra, submarinos lanzamisiles y plataformas aéreas estratégicas— representa uno de los entornos más sensibles para el equilibrio disuasivo global.

Las tensiones derivadas del conflicto en Ucrania desde 2022 y la respuesta adaptativa de la OTAN han modificado sustancialmente el entorno estratégico euroatlántico. Rusia ha priorizado el refuerzo de su disuasión nuclear y ha invertido en la modernización de su red NC3, integrando capacidades cibernéticas y de inteligencia artificial en los sistemas de alerta y mando. Paralelamente, la Alianza Atlántica ha acelerado su doctrina de ciberdefensa avanzada, creando estructuras de coordinación como el *NATO CyOC* (*Cyber Operations Centre*) y ampliando los programas de interoperabilidad entre los Estados miembro.

En este escenario de rivalidad tecnológica, la comprensión de los riesgos cibernéticos asociados a la tríada nuclear rusa se convierte en una tarea fundamental para la seguridad internacional, especialmente desde el punto de vista preventivo y doctrinal. La escasez de información pública sobre estos sistemas, unida al carácter reservado de la mayor parte de las infraestructuras de mando y control, obliga a adoptar metodologías alternativas basadas en fuentes abiertas verificadas (OSINT), marcos de riesgo reconocidos como NIST 800-30 e ISO/IEC 27005, y técnicas de modelización que permitan extrapolar comportamientos teóricos sin comprometer información clasificada.

En este sentido, el presente trabajo no pretende identificar vulnerabilidades específicas ni describir estructuras técnicas concretas, sino ofrecer un modelo metodológico reproducible para analizar el riesgo cibernético y la resiliencia doctrinal en infraestructuras críticas de mando nuclear. Este enfoque permite aproximarse al fenómeno desde una perspectiva científica, auditable y de utilidad práctica para instituciones académicas, centros de pensamiento estratégico y organismos de defensa que operan en entornos de información restringida.

La novedad de la investigación reside en tres aspectos principales:

1. La aplicación sistemática del marco NIST 800-30 a un dominio tradicionalmente reservado a la inteligencia clasificada.
2. La incorporación del concepto de resiliencia estratégica entendida no solo como la capacidad de resistir un ciberataque, sino de mantener la estabilidad doctrinal y operativa ante un entorno digital hostil.
3. La formulación de un modelo analítico abierto, verificable y replicable, que permite futuras investigaciones interdisciplinarias sin comprometer la seguridad de la información.

En última instancia, este estudio busca contribuir al debate sobre la estabilidad disuasiva en la era digital, proponiendo un marco conceptual y metodológico que facilite la cooperación científica y tecnológica entre aliados, y fomente la cultura de prevención, disuasión y respuesta frente a amenazas tecnológicas de nueva generación.

El apartado siguiente describe la metodología adoptada, los criterios de selección documental y el proceso de codificación temática aplicado para la construcción del modelo de análisis.

2 Marco metodológico y fuentes

El estudio se sustenta en una metodología rigurosa, diseñada para garantizar la validez científica del análisis sin vulnerar restricciones de seguridad ni revelar información clasificada. Dado que la investigación aborda un ámbito de alta sensibilidad —el sistema de mando, control y comunicaciones nucleares (NC3) ruso—, se opta por un método mixto y reproducible que combina la revisión sistemática de literatura, la codificación temática y la modelización de escenarios de riesgo bajo estándares internacionales de gestión cibernética. Este enfoque permite desarrollar un marco analítico verificable a partir de fuentes abiertas, estructurado en fases que van desde la selección documental hasta la validación metodológica del modelo.

2.1 Enfoque general

El presente estudio adopta un enfoque mixto, cualitativo-cuantitativo, orientado al análisis del riesgo cibernético en infraestructuras estratégicas de mando, control y comunicaciones nucleares (NC3). Dada la naturaleza reservada del objeto de estudio, se recurre a una metodología basada en la triangulación de fuentes abiertas verificadas, marcos internacionales de gestión del riesgo y técnicas de inferencia conceptual.

Antes de desarrollar cada fase, se sintetiza el proceso metodológico seguido en la tabla I, que muestra la secuencia de análisis y las normas de referencia aplicadas.

TABLA I. FASES METODOLÓGICAS Y MARCOS DE REFERENCIA APLICADOS

Fase	Objetivo analítico	Herramienta / Referencia	Resultado esperado
1 Revisión documental sistemática	Identificar literatura institucional y académica sobre NC3, ciberseguridad y resiliencia estratégica (2018-2025).	Protocolo PRISMA 2020. Bases: RAND, NATO STO, SIPRI, IISS, Chatham House.	Corpus verificado de fuentes abiertas (58 documentos).
2 Codificación temática	Agrupar hallazgos en tres ejes: vulnerabilidad estructural, digitalización estratégica y respuesta doctrinal.	Análisis de contenido inductivo.	Matriz de indicadores de riesgo y resiliencia.
3 Modelización de escenarios de riesgo	Simular posibles vectores de interferencia o degradación del NC3 desde un punto de vista teórico.	NIST SP 800-30 Rev. 1 (2012); ISO/IEC 27005 (2018).	Escenarios conceptuales de exposición y resiliencia.
4 Evaluación del impacto estratégico	Valorar la afectación potencial sobre la estabilidad disuasiva y la cooperación euroatlántica.	Escala semicuantitativa (probabilidad × impacto).	Mapa de riesgo estratégico (teórico).
5 Síntesis y validación metodológica	Comprobar la coherencia del modelo con la doctrina aliada de ciberdefensa.	Cross-check RAND–NATO STO–SIPRI.	Marco metodológico reproducible y auditable.

Fuente: elaboración propia a partir de NIST 800-30 (2012) e ISO/IEC 27005 (2018).

2.2 Selección y validación del corpus documental

La base empírica inicial estuvo compuesta por trescientos doce documentos obtenidos de bases institucionales y centros de pensamiento especializados —entre ellos, RAND (*Research and Development Corporation*), SIPRI (*Stockholm International Peace Research Institute*), NATO STO (*Science and Technology Organization*), CSIS (*Center for Strategic and International Studies*), IISS (*International Institute for Strategic Studies*), Chatham House y Carnegie Endowment—, seleccionados por su relevancia y rigor analítico. Tras aplicar criterios de relevancia temática, autenticidad institucional y ausencia de duplicados, el corpus se redujo a 58 referencias principales.

Se empleó el protocolo PRISMA 2020 (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), una guía internacional para la elaboración transparente y reproducible de revisiones sistemáticas, con el fin de depurar las fuentes y garantizar su trazabilidad metodológica. Posteriormente, se aplicó una codificación temática inductiva, que permitió agrupar los hallazgos en tres ejes de análisis:

a) Vulnerabilidades estructurales del NC3;

b) riesgos derivados de la digitalización estratégica y la inteligencia artificial;

c) respuestas doctrinales y marcos de resiliencia en el entorno euroatlántico.

Cada documento fue registrado en un anexo documental con URL verificadas y metadatos básicos (autor, año, fuente institucional, tipo de documento), garantizando la verificabilidad y reproducibilidad del proceso.

Las fuentes utilizadas se clasificaron en cuatro categorías principales:

1. Documentos doctrinales y técnicos emitidos por organismos internacionales (OTAN, ONU, Unión Europea, Ministerio de Defensa de la Federación Rusa).
2. Informes de centros de pensamiento y organismos de investigación estratégica (RAND, NATO STO, SIPRI, IISS, Chatham House).
3. Literatura académica y científica indexada en bases como Scopus, Web of Science y Dialnet Plus.
4. Fuentes periodísticas verificadas, utilizadas solo para contextualizar desarrollos recientes (2022-2025) sobre modernización de misiles y doctrinas de mando.

La autenticidad de cada documento se contrastó mediante verificación cruzada de procedencia institucional, fecha de emisión, citación bibliográfica y disponibilidad pública. Esta validación garantiza que las fuentes OSINT empleadas mantengan criterios de trazabilidad, actualidad y fiabilidad, cumpliendo los estándares de transparencia exigidos por la investigación científica en materia de defensa.

2.3 Aplicación del modelo NIST 800-30 e ISO/IEC 27005

El análisis del riesgo siguió la estructura propuesta por la guía NIST SP 800-30 (*Guide for Conducting Risk Assessments*, elaborada por el *National Institute of Standards and Technology* de EE. UU.), adaptada al contexto estratégico de defensa. Este marco

proporciona un procedimiento estandarizado para identificar, estimar y priorizar riesgos tecnológicos en sistemas críticos:

1. Identificación de activos y funciones críticas del NC3 (sin detallar plataformas ni protocolos).
2. Caracterización de amenazas según tipología cibernética: interferencias en comunicaciones, sabotaje de software, manipulación de sensores y desinformación cognitiva.
3. Estimación de probabilidad e impacto de cada amenaza sobre la estabilidad estratégica mediante una escala semicuantitativa.
4. Determinación del riesgo residual y formulación de estrategias de mitigación.

De forma complementaria, se aplicó la norma ISO/IEC 27005, emitida por la *International Organization for Standardization* y la *International Electrotechnical Commission*, que ofrece directrices para la gestión del riesgo en seguridad de la información. Su integración permite incorporar la dimensión organizacional y doctrinal de la resiliencia, alineando el análisis técnico con los principios de gobernanza y control operativo. El resultado es un modelo reproducible de análisis del riesgo cibernético estratégico, aplicable a infraestructuras críticas con acceso limitado a información clasificada.

2.4 Justificación del uso de fuentes abiertas (OSINT)

Lejos de constituir una limitación, la dependencia de fuentes abiertas representa una ventaja metodológica en términos de transparencia, seguridad y cooperación científica. El uso de OSINT permite:

– Validar hipótesis mediante información verificable y accesible.
– Respetar los márgenes de confidencialidad operativa.
– Favorecer la colaboración académica y doctrinal entre aliados.

De este modo, la restricción informativa se convierte en una condición epistemológica legítima, donde la innovación se centra en el modelo de análisis, no en la exposición de datos sensibles. Así, el estudio contribuye a consolidar un lenguaje metodológico común para el examen del riesgo cibernético en entornos estratégicos y para la interacción entre el ámbito académico y las instituciones de defensa.

2.5 Limitaciones y perspectivas futuras

Se reconoce que el uso exclusivo de OSINT impide la contrastación empírica directa con datos clasificados. No obstante, el modelo desarrollado puede ser extendido y validado por investigadores con acceso restringido, lo que garantiza su escalabilidad.

Futuras líneas de investigación incluyen la aplicación de aprendizaje automático (*machine learning*) para detectar patrones de riesgo y el análisis comparativo de resiliencia cibernética entre doctrinas NC3 de distintas potencias nucleares.

En conjunto, este marco metodológico ofrece una base científica y reproducible para estudios futuros sobre ciberseguridad estratégica y resiliencia en sistemas de mando nuclear.

3 Marco teórico y conceptual

La comprensión del riesgo cibernético en la tríada nuclear rusa exige articular una base teórica que combine los enfoques doctrinales clásicos de la disuasión con los nuevos paradigmas de seguridad digital y resiliencia tecnológica. Este apartado establece las *fundaciones conceptuales* que sustentan el análisis posterior, integrando aportaciones procedentes de la literatura académica, los informes de investigación estratégica y los marcos normativos internacionales sobre gestión del riesgo cibernético (ISO/IEC, 2022; Joint Task Force, 2018).

El propósito de este marco no es revelar estructuras específicas de mando, sino ofrecer un modelo interpretativo que permita entender cómo la digitalización del sistema NC3 ruso puede incidir en la estabilidad estratégica global. Desde esta perspectiva, la teoría de la disuasión, los estudios sobre riesgo nuclear y los desarrollos doctrinales en ciberdefensa convergen para explicar un escenario en transformación, donde el riesgo tecnológico se convierte en un vector geopolítico de primer orden (Johnson, 2021; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

El propósito de este marco no es revelar estructuras específicas de mando, sino ofrecer un modelo interpretativo que permita entender *cómo la digitalización del sistema NC3 ruso puede incidir en la estabilidad estratégica global*. Desde esta perspectiva, la teoría de la disuasión, los estudios sobre riesgo nuclear y los desarrollos doctrinales en ciberdefensa convergen para explicar un escenario en transformación, donde el riesgo tecnológico se convierte en un vector geopolítico de primer orden (Johnson, 2021; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

3.1 Fundamentos de la tríada nuclear y el sistema NC3

La tríada nuclear constituye el núcleo de la disuasión estratégica moderna. Diseñada para asegurar la capacidad de segundo ataque, se compone de tres componentes complementarios: misiles balísticos intercontinentales (ICBM), misiles balísticos lanzados desde submarinos (SLBM) y bombarderos estratégicos (Kristensen y Korda, 2023). La lógica de la tríada es mantener una disuasión creíble mediante la supervivencia del arsenal frente a un ataque preventivo, concepto que sigue siendo esencial en la doctrina rusa actual (IISS, 2023). Los datos comparativos de fuerzas y programas de modernización respaldan esta configuración de la tríada rusa (IISS, 2024).

El sistema Nuclear Command, Control and Communications (NC3) integra las funciones de mando político, control operacional y transmisión de órdenes hacia las fuerzas nucleares. Según Acton (2018), la confiabilidad del NC3 es la condición *sine qua non* de la estabilidad nuclear global: cualquier degradación o ambigüedad en su funcionamiento podría generar una crisis de percepción o una escalada accidental.

El NC3 ruso ha evolucionado desde la arquitectura soviética (*Kazbek System*, *Cheget*) hacia una red más automatizada, apoyada en satélites GLONASS y comunicaciones cifradas redundantes (CSIS, 2024; Mazarr *et al* , 2022). Sin embargo, la interconexión digital y la introducción de inteligencia artificial en los procesos de decisión también amplían la superficie de exposición ante interferencias o ciberataques (Kristensen y Korda, 2022b).

Esta evolución tecnológica plantea la necesidad de evaluar los riesgos asociados a la digitalización del NC3. Comprender la naturaleza y las dimensiones del riesgo cibernético en sistemas estratégicos se convierte así en el paso lógico siguiente para interpretar las vulnerabilidades inherentes al modelo de disuasión contemporáneo.

3.2 Riesgo cibernético en sistemas estratégicos

El riesgo cibernético se define como la probabilidad de que una acción o vulnerabilidad digital afecte la integridad, confidencialidad o disponibilidad de un sistema crítico (Joint Task Force, 2018). En el dominio nuclear, este riesgo trasciende el plano técnico: puede alterar la confianza entre Estados y desestabilizar los equilibrios de disuasión.

Los estudios del *Carnegie Endowment for International Peace* y del *SIPRI* destacan que los incidentes cibernéticos en infraestructuras estratégicas pueden generar «efectos catalíticos», es decir, desencadenar reacciones desproporcionadas por percepciones erróneas del adversario (Jung, 2024;Kristensen y Korda, 2022b); Mazarr *et al* (2022) y CSIS (2024) coinciden en que el NC3 ruso, pese a su redundancia, enfrenta riesgos crecientes vinculados a la automatización de sensores, la dependencia de software propietario y el acceso remoto a nodos de decisión.

De acuerdo con estos estudios, los principales vectores de amenaza se agrupan en cuatro categorías:

1. Intrusión digital o manipulación de *firmware* en nodos de comunicación estratégica.
2. Interferencia electromagnética o de señal satelital, que afecta la fiabilidad de la alerta temprana.
3. Operaciones de desinformación y ciberengaño dirigidas a la cadena de mando político-militar.
4. Dependencia tecnológica y vulnerabilidad de la cadena de suministro, en especial de componentes microelectrónicos importados.

Estas amenazas, documentadas en informes del *NATO STO* (2023) y del *IISS* (2023), ilustran cómo la digitalización estratégica transforma los riesgos clásicos de disuasión en desafíos multidimensionales que combinan ciberseguridad, inteligencia y psicología estratégica.

El análisis de estos vectores de riesgo conduce necesariamente al examen de las capacidades de resiliencia. Si el riesgo representa el grado de exposición, la resiliencia

determina la capacidad del sistema para mantener sus funciones críticas bajo ataque o perturbación. Este cambio de enfoque resulta clave para comprender la estabilidad en el entorno nuclear digital.

3.3 Resiliencia estratégica y ciberestabilidad

El concepto de resiliencia estratégica ha evolucionado desde una noción técnica hacia un principio doctrinal que define la capacidad de los Estados para mantener funciones esenciales bajo presión o ataque (Payne, 2022). En el contexto cibernético, implica no solo resistir una agresión, sino asegurar la continuidad operativa, la adaptabilidad organizativa y la recuperación rápida del sistema afectado.

La OTAN formalizó esta visión tras la Cumbre de Varsovia (2016) y la reafirmó en su *Strategic Concept 2022*, reconociendo el ciberespacio como un dominio operativo. Su *Cyber Defence Pledge* y el marco de investigación del *NATO Science and Technology Organization* (U.S. Department of Defense, 2020) promueven la integración de resiliencia digital en la planificación de defensa.

Rusia, por su parte, desarrolla desde 2020 una doctrina de «estabilidad informacional», que combina la defensa cibernética con el control de la información y la redundancia técnica de los sistemas NC3 (CSIS, 2024). Esta visión se centra en mantener la autonomía tecnológica y reducir la exposición a vulnerabilidades externas.

El paso de la resiliencia técnica a la resiliencia estratégica introduce un nuevo componente: la *ciberdisuasión*. Si la resiliencia garantiza la supervivencia del sistema, la disuasión asegura la previsibilidad del adversario. Ambas se complementan en un marco donde la estabilidad depende tanto de la fortaleza tecnológica como de la percepción de credibilidad.

3.4 Ciberdisuasión y estabilidad estratégica

La transformación digital de la disuasión nuclear ha impulsado el surgimiento del concepto de ciberdisuasión, entendido como la capacidad de prevenir agresiones mediante la protección robusta de infraestructuras críticas y la credibilidad de las respuestas ante ataques (Johnson, 2021).

Autores como Futter (2018) y Morgan (2023) argumentan que la disuasión tradicional —basada en el miedo a la destrucción mutua asegurada— se está desplazando hacia una «disuasión por resiliencia», donde la fortaleza del sistema y su capacidad de absorber un ataque sin perder funcionalidad son factores decisivos.

La estabilidad estratégica contemporánea se define, por tanto, no solo por la cantidad o potencia del arsenal nuclear, sino por la robustez cibernética del NC3. Los informes de RAND (2025) y SIPRI (2024) advierten que la vulnerabilidad digital en redes de mando nuclear podría convertirse en el principal catalizador de inestabilidad si no se adoptan medidas coordinadas de prevención, cooperación y transparencia tecnológica entre las potencias.

Este conjunto de conceptos —riesgo, resiliencia y ciberdisuasión— configura la base del modelo analítico empleado en la presente investigación. A partir de ellos, se establece un marco conceptual integrador que vincula la seguridad tecnológica con la estabilidad estratégica, sirviendo de soporte a la discusión de resultados.

3.5 Síntesis del marco conceptual

El marco teórico de este estudio se sostiene sobre cuatro ejes fundamentales:

1. La tríada nuclear, como estructura de disuasión clásica y garante del equilibrio estratégico (Kristensen y Korda, 2023).
2. El sistema NC3, como núcleo técnico y doctrinal de la comunicación nuclear (Jung, 2024; CSIS, 2024).
3. El riesgo cibernético, que introduce incertidumbre tecnológica y estratégica (Joint Task Force, 2018; SIPRI, 2024).
4. La resiliencia estratégica, que transforma la ciberseguridad en elemento de estabilidad (Payne, 2022; U.S. Department of Defense, 2020).

Estos conceptos conforman un marco integrador que permite examinar los niveles de exposición y recuperación del NC3 ruso en el contexto de la competencia tecnológica global.

A continuación, se presenta un Glosario de términos y acrónimos básicos (Sección 4), con el fin de facilitar la comprensión de los conceptos técnicos, doctrinales y tecnológicos empleados en la investigación.

Posteriormente, la Sección 5 desarrolla los resultados del análisis, organizados en torno a los tres ejes identificados: vulnerabilidad estructural, digitalización estratégica y respuesta doctrinal.

4 Glosario de términos y acrónimos básicos

El presente glosario ofrece definiciones sintéticas de los principales conceptos técnicos y doctrinales empleados a lo largo del artículo. Su objetivo es facilitar la comprensión de la terminología especializada vinculada con la ciberseguridad estratégica, la disuasión nuclear y los sistemas de mando y control (NC3), evitando que el lector deba recurrir a fuentes externas.

La inclusión de este apartado responde a la recomendación de los revisores de proporcionar un marco de referencia terminológico temprano, que permita una lectura fluida y coherente de los apartados posteriores. Las definiciones presentadas combinan criterios técnicos, doctrinales y científicos, y se han elaborado a partir de literatura académica indexada y fuentes institucionales reconocidas (Jung, 2024; Futter, 2018; Kristensen y Korda, 2023; Payne, 2022; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

TABLA A. GLOSARIO DE TÉRMINOS Y ACRÓNIMOS BÁSICOS

Término / Acrónimo	Definición académica resumida	Aplicación en el estudio
NC_3 (*Nuclear Command, Control and Communications*)	Conjunto de sistemas, redes y procedimientos que permiten a las autoridades nacionales controlar y comunicar órdenes sobre el uso de armas nucleares.	Núcleo funcional de la disuasión nuclear rusa analizada en este estudio.
Tríada nuclear	Estructura compuesta por tres plataformas de lanzamiento: misiles intercontinentales terrestres (ICBM), misiles lanzados desde submarinos (SLBM) y vectores aéreos estratégicos.	Marco estructural para la evaluación del riesgo cibernético en cada dominio.
ICBM (Intercontinental Ballistic Missile)	Misil balístico con alcance superior a 5500 km, capaz de transportar cabezas nucleares entre continentes.	Uno de los tres componentes analizados en la tríada rusa.
SLBM (*Submarine-Launched Ballistic Missile*)	Misil balístico lanzado desde submarinos de propulsión nuclear, parte esencial de la capacidad de segundo golpe.	Representa la dimensión naval del NC_3 ruso.
Segundo golpe (*Second Strike*)	Capacidad de un Estado para responder con armas nucleares tras haber sufrido un ataque inicial.	Indicador central de la estabilidad estratégica y del impacto del riesgo cibernético.
Ciberdisuasión (*Cyber Deterrence*)	Estrategia destinada a prevenir ataques informáticos mediante resiliencia, atribución y capacidad de respuesta proporcional.	Concepto empleado para evaluar la respuesta OTAN-Ucrania frente a ciberamenazas estratégicas.
Ciberresiliencia	Capacidad de un sistema para resistir, adaptarse y recuperarse ante un ataque cibernético manteniendo funciones críticas.	Objetivo operativo de refuerzo en los sistemas NC_3.
OSINT (*Open Source Intelligence*)	Inteligencia obtenida a partir de fuentes abiertas, verificables y accesibles públicamente, utilizada con fines de análisis estratégico o científico.	Base metodológica que garantiza la transparencia y reproducibilidad de la investigación.
NIST (*National Institute of Standards and Technology*)	Organismo estadounidense que desarrolla estándares técnicos y metodológicos, entre ellos la serie *Special Publication 800-30* para análisis de riesgos.	Referencia metodológica principal para la modelización de riesgo cibernético.
ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*)	Entidades internacionales que emiten normas conjuntas sobre gestión de seguridad de la información y riesgo tecnológico (ISO/IEC 27005).	Marco complementario al NIST para la evaluación de resiliencia organizacional.
Spoofing	Manipulación o suplantación de señales electrónicas —especialmente GNSS o satelitales— con el fin de alterar datos de navegación o localización.	Riesgo técnico identificado en los sistemas de guiado SLBM y vectores aéreos.
Firmware	*Software* de bajo nivel que controla el funcionamiento del *hardware* y establece la interfaz entre equipos y programas.	Superficie de ataque potencial en los sistemas de control y lanzamiento.
GLONASS	Sistema global de navegación por satélite de la Federación Rusa, equivalente al GPS.	Dependencia tecnológica crítica para sincronización y guiado.
Perimetr	Sistema automatizado de mando ruso diseñado para garantizar la represalia nuclear incluso ante pérdida de comunicación con el mando político.	Ejemplo doctrinal de automatización con riesgo cibernético inherente.
Zero Trust	Modelo de seguridad que elimina la confianza implícita dentro de las redes internas, verificando cada acceso o transacción.	Principio recomendado para modernizar la seguridad del NC_3 ruso y aliado.

Fuente: elaboración propia a partir de Jung (2024), Futter (2018), Harknett y Smeets (2020), Kristensen y Korda (2023), Payne (2022), Mazarr *et al* (2022), Joint Task Force (2018), ISO/IEC (2018) y U.S. Department of Defense (2020). Las definiciones sintetizan terminología técnica estandarizada en doctrina nuclear y ciberseguridad

El presente glosario constituye una referencia conceptual que enmarca el análisis técnico y estratégico desarrollado en las secciones siguientes. Al clarificar la terminología esencial, se busca garantizar que el lector interprete de forma homogénea los términos doctrinales, técnicos y operativos empleados en el estudio.

La siguiente sección expone los resultados y el análisis técnico-derivados de la aplicación del modelo metodológico, organizados en torno a los tres ejes de investigación definidos: vulnerabilidad estructural, digitalización estratégica y respuesta doctrinal.

5 Resultados y análisis técnico

El estudio se centró en los tres componentes de la tríada nuclear rusa —misiles balísticos intercontinentales (ICBM), misiles balísticos lanzados desde submarinos (SLBM) y vectores aéreos estratégicos—, examinando las interacciones entre los subsistemas de comunicación, guiado y control. Este enfoque multidimensional permitió determinar la exposición diferencial al riesgo cibernético en cada dominio operativo.

Entre los sistemas evaluados, el RS-24 Yars constituye un caso paradigmático por su relevancia estratégica y su grado de digitalización, lo que lo convierte en un modelo de referencia para comprender la convergencia entre tecnología, doctrina y vulnerabilidad.

5.1 El RS-24 Yars como modelo técnico de referencia

Antes de presentar los resultados cuantitativos, resulta necesario contextualizar el modelo técnico que sirve como base del análisis empírico. El RS-24 Yars representa el vector terrestre principal de la tríada rusa y ejemplifica la complejidad de las cadenas de mando y control digitales asociadas a los ICBM.

La figura 1, que se muestra a continuación, ilustra la configuración estructural y la relevancia del componente terrestre del sistema NC3, destacando la criticidad del *firmware* y los módulos de guiado como posibles superficies de exposición cibernética.

Figura 1. Sistema de misiles balísticos intercontinentales RS-24 Yars.
Nota: el RS-24 Yars constituye el principal ICBM de la tríada nuclear rusa. Su arquitectura digital y sus sistemas de guiado automatizados evidencian la vulnerabilidad potencial del firmware y las redes de comunicación de control. *Fuente*: GlobalSecurity.org (s. f.). RS-24 Yars Intercontinental Ballistic Missile.

El RS-24 Yars (*PC-24 «Ярс»*; designación OTAN SS-27 Mod 2) es un misil balístico intercontinental (ICBM) de combustible sólido, con un alcance aproximado de 12 800 km y múltiples ojivas termonucleares MIRV (100–550 kt). En servicio desde 2010, puede ser lanzado desde silos fijos o plataformas móviles TEL (*Transporter-Erector-Launcher*), diseñadas para asegurar la movilidad y supervivencia del sistema. Evoluciona del *Topol-M* y fue diseñado para superar los sistemas de defensa antimisiles contemporáneos, incorporando algoritmos de guiado autónomo y redundancia digital (Kristensen y Korda, 2023; IISS, 2023).

Su integración en redes digitales y su dependencia de canales de comunicación cifrados convierten al RS-24 en un objeto de análisis prioritario dentro del sistema NC3 ruso. A partir de este modelo, se desarrollaron dos niveles complementarios de evaluación:

1. Análisis cronológico y cualitativo (2020-2025): cronología de incidentes tecnológicos y cibernéticos relevantes.
2. Modelización de riesgo NIST 800-30: cuantificación del riesgo relativo combinando probabilidad (P) e impacto (I).

A partir de los hallazgos obtenidos en el análisis cualitativo, se presenta a continuación la cronología verificada de incidentes tecnológicos y cibernéticos (2020-2025), con el fin de contextualizar la evolución del riesgo antes de su modelización cuantitativa.

5.2 Cronología de incidentes y vulnerabilidades (2020-2025)

La cronología que se muestra a continuación resume los incidentes relevantes asociados a fallos tecnológicos o ciberataques que potencialmente afectaron al NC3 ruso. Cada registro fue validado mediante verificación cruzada de fuentes académicas, think tanks y organismos internacionales (SIPRI, 2024; RAND Corporation, 2021; CSIS, 2024; U.S. Department of Defense, 2020; IISS, 2023).

Tras el análisis del sistema RS-24 Yars como modelo representativo, resulta pertinente situar los hallazgos dentro de una secuencia temporal de incidentes tecnológicos y cibernéticos que permita contextualizar la evolución del riesgo.

La tabla II permite observar la progresión de los riesgos y la evolución de las amenazas en el tiempo, aportando una base empírica para la identificación de patrones recurrentes.

TABLA II. CRONOLOGÍA RESUMIDA DE INCIDENTES TECNOLÓGICOS Y CIBERNÉTICOS (2020–2025)

Fecha	Sistema / Dominio	Descripción del incidente o vulnerabilidad detectada	Tipo de vulnerabilidad
Mar. 2020	Infraestructura NC3 terrestre	Ataques DDoS contra servidores del Ministerio de Defensa ruso, filtraciones parciales de credenciales.	Intrusión en red
Jul. 2021	Segmento GNSS (GLONASS)	Episodios de spoofing en el Mar Negro que afectaron a aeronaves y buques civiles; posible ensayo de contramedidas.	Manipulación de señal

Fecha	Sistema / Dominio	Descripción del incidente o vulnerabilidad detectada	Tipo de vulnerabilidad
Feb. 2022	Sistemas ICBM (Yars)	Actualización de firmware retrasada por alertas de incompatibilidad en protocolos de criptografía.	Fallo de *software*
Dic. 2022	Vectores aéreos (Tu-95MS)	Malfunción del sistema de comunicación HF durante simulacro estratégico.	Vulnerabilidad en comunicaciones
Abr. 2023	Red de alerta temprana (Oko)	Anomalías en telemetría satelital por *software* obsoleto.	Obsolescencia digital
Oct. 2023	Submarinos Borei	Corte temporal en enlace satélite «Legenda» durante maniobras árticas.	Interferencia en comunicaciones
Mar. 2024	Infraestructura de mando y control	Filtración de datos en plataformas logísticas militares digitales.	Compromiso de cadena de suministro
Ene. 2025	Sistema de ensayo *Avangard*	Latencias en red de telemetría por configuración deficiente de *routers* militares.	Fallo de configuración

Fuente: elaboración propia a partir de SIPRI (2022; 2024), RAND Corporation (2024-2025), NATO STO (2023), CSIS (2021, 2024) e IISS (2023).

El análisis de esta cronología permite inferir tres patrones de exposición tecnológica persistentes, vinculados con la dependencia satelital, la segmentación deficiente de redes y la vulnerabilidad de las cadenas logísticas.

5.2.1 Vulnerabilidades específicas en la Armada y la Aviación estratégicas rusas

Además de los vectores terrestres, los dominios naval y aéreo del sistema NC3 ruso presentan vulnerabilidades diferenciadas que amplían el espectro del riesgo cibernético.

La flota estratégica de submarinos clase *Borei*, equipada con misiles RSM-56 *Bulava*, depende de los enlaces satelitales «Legenda» y de transmisiones en frecuencia extremadamente baja VLF (*Very Low Frequency*), utilizadas para mantener comunicación con submarinos sumergidos, canales cuya fiabilidad se ha visto comprometida por interferencias y *spoofing* (manipulación o suplantación de señales electrónicas) documentados en ejercicios árticos (Mazarr *et al.*, 2022; SIPRI, 2024). Estas vulnerabilidades, unidas a la dificultad de actualización en entornos submarinos, reducen la capacidad de detección temprana y comunicación de órdenes críticas. Las tendencias de modernización y dependencias tecnológicas de plataformas estratégicas están documentadas en *The Military Balance 2024* (IISS, 2024).

En el dominio aéreo, los bombarderos estratégicos *Tu-95MS* y *Tu-160* utilizan misiles de crucero *Kh-55/Kh-102* y enlaces HF/UHF susceptibles de interferencias electromagnéticas y manipulación de coordenadas GNSS, lo que puede afectar la precisión de lanzamiento y la transmisión de comandos (IISS, 2024). La coexistencia de sistemas analógicos y digitales en estas aeronaves incrementa la complejidad del aseguramiento cibernético y exige redundancia manual como mecanismo de control positivo.

Por su parte, los sistemas hipersónicos Avangard y Kinzhal, de acuerdo con informes de la DARPA (*Defense Advanced Research Projects Agency*), presentan velocidades y niveles de automatización que incrementan significativamente la

complejidad del control. Al depender de redes de guiado en tiempo real y enlaces de telemetría cifrados, incorporan un nuevo nivel de riesgo: la posible pérdida de control humano directo en caso de fallos de sincronización o degradación del enlace satelital. La velocidad y automatización de dichos sistemas hace que un error en la cadena de mando digital pueda generar consecuencias estratégicas desproporcionadas.

De manera global, los resultados confirman que la cibervulnerabilidad del NC3 ruso se extiende a los tres dominios —terrestre, naval y aéreo—, y que la resiliencia tecnológica debe evaluarse considerando las particularidades de cada vector operativo.

En el siguiente apartado, se examinan estas recurrencias en detalle, con base en la clasificación del modelo NIST.

5.3 Aplicación de la matriz NIST 800-30: modelización de riesgo

Antes de exponer la tabla de modelización, resulta pertinente sintetizar los patrones recurrentes detectados en los incidentes documentados. Este paso intermedio facilita la interpretación comparada de riesgos y evita la fragmentación de los resultados.

El examen cruzado de los eventos registrados identifica tres categorías dominantes de exposición cibernética:

1. Dependencia GNSS y comunicaciones satelitales: el riesgo derivado del *spoofing* o interferencia en GLONASS afecta la integridad de la navegación y sincronización estratégica (SIPRI, 2024).
2. Obsolescencia y segmentación deficiente de redes: los sistemas NC3 heredados mezclan componentes analógicos y digitales, dificultando la implementación de entornos *Zero Trust* (Mazarr *et al.*, 2022).
3. Amenazas en la cadena de suministro: la incorporación de *software* civil o de proveedores externos incrementa la superficie de ataque en componentes críticos (CSIS, 2024; U.S. Department of Defense, 2020).

Estas tipologías se corresponden con las categorías de riesgo técnico descritas por el Joint Task Force (2018): *hardware*, *software* y procedimientos organizativos.

Una vez definidos los patrones, se aplicó la matriz NIST 800-30 para estimar la probabilidad e impacto de cada tipo de vulnerabilidad, obteniendo una cuantificación del riesgo relativo (R=P × I).

La aplicación del modelo NIST al conjunto del sistema NC3 ruso se ha extendido a los dominios naval y aéreo descritos en el epígrafe anterior.

Las vulnerabilidades detectadas en los submarinos *Borei* (dependencia de enlaces VLF y satelitales) y en los bombarderos estratégicos *Tu-95MS* y *Tu-160* (exposición a interferencias GNSS y fallos de comunicación HF/UHF) reflejan patrones de riesgo sistémico similares a los identificados en los vectores terrestres.

En consecuencia, el modelo de probabilidad e impacto se amplía para incluir variables de entorno operativo —profundidad, latencia de señal y automatización— que condicionan la respuesta ante un evento cibernético.

Esta integración permite cuantificar de forma más precisa la exposición transversal del NC3 en sus tres componentes (terrestre, naval y aéreo), asegurando coherencia con el principio de ciber-resiliencia estructural definido por el NIST (2023) y la NATO STO (2024).

La matriz actualizada (tabla III) incorpora, además, las vulnerabilidades detectadas en las plataformas submarinas y aéreas, siguiendo los criterios de probabilidad e impacto del modelo NIST 800-30.

TABLA III. MATRIZ NIST 800-30 AMPLIADA PARA EL NC3 RUSO (MULTIDOMINIO)

Escenario de riesgo	Probabilidad (P)	Impacto (I)	Riesgo relativo (R=P × I)	Nivel de riesgo	Efecto doctrinal estimado
1 *Spoofing* de GLONASS en SLBM	4	4	16	Alto	Desviación de trayectoria; degradación de credibilidad de segundo golpe.
2 Infiltración de *firmware* en ICBM	3	5	15	Alto	Riesgo de fallo de lanzamiento o bloqueo no autorizado de sistemas.
3 Intrusión en red NC3 centralizada	2	5	10	Medio-alto	Pérdida temporal de comunicaciones estratégicas.
4 Compromiso de cadena de suministro	3	3	9	Medio	Alteración de módulos logísticos digitales con retraso en mantenimiento.
5 Obsolescencia de *software* en radares de alerta temprana	4	2	8	Medio	Retraso en detección de lanzamientos hostiles.
6 Interferencia en comunicaciones VLF/ satélite de submarinos Borei (RSM-56 Bulava)	3	5	15	Alto	Riesgo de aislamiento temporal del mando naval, pérdida parcial de capacidad de represalia.
7. *Spoofing* GNSS e interferencia electromagnética en bombarderos Tu-95MS/Tu-160 (misiles Kh-55/Kh-102)	4	4	16	Alto	Desviación de blancos o fallos de enlace; erosión de control positivo y fiabilidad de comando aéreo.

Fuente: elaboración propia a partir de NIST (2023), RAND Corporation (2024), SIPRI (2024), IISS (2024) y NATO Science and Technology Organization (2024). Los valores de probabilidad (P) e impacto (I) se expresan en escala ordinal (1=bajo, 5=muy alto). Los escenarios 6 y 7 representan la extensión multidominio del modelo a las plataformas navales y aéreas del NC3 ruso.

A partir de los valores obtenidos en la tabla III, se derivan patrones de riesgo que permiten evaluar de forma integrada la relación entre vulnerabilidades técnicas y credibilidad disuasiva. Estos hallazgos se sintetizan en el apartado siguiente.

En conjunto, estas evidencias permiten transitar del análisis empírico a la modelización cuantitativa del riesgo, donde la matriz NIST 800-30 ofrece una visión integrada de la exposición tecnológica y la resiliencia del sistema NC3.

5.4 Síntesis de resultados

A partir de los valores obtenidos en la tabla III, se derivan tendencias significativas que permiten interpretar la vulnerabilidad cibernética del sistema NC3 ruso desde una perspectiva multidominio.

El análisis confirma que los factores de riesgo no se distribuyen de manera homogénea, sino que responden a la naturaleza específica de cada componente de la tríada nuclear: terrestre (ICBM), naval (SLBM) y aéreo (vectores estratégicos tripulados).

En el dominio terrestre, la exposición se concentra en las infiltraciones de *firmware* y la obsolescencia de *software*, lo que refleja la persistencia de arquitecturas híbridas con escasa segmentación de red.

En el dominio naval, la interferencia en comunicaciones VLF y satelitales de los submarinos *Borei* (equipados con misiles *RSM-56 Bulava*) constituye el riesgo más relevante, ya que podría aislar temporalmente la cadena de mando y comprometer la capacidad de segundo golpe.

Finalmente, en el dominio aéreo, la dependencia de enlaces GNSS y HF/UHF en bombarderos estratégicos *Tu-95MS* y *Tu-160*, junto con sus misiles *Kh-55* y *Kh-102*, introduce una vulnerabilidad crítica ante ataques de spoofing o interferencias electromagnéticas.

De forma transversal, los resultados muestran que los riesgos de comunicación y sincronización satelital son los más críticos para la estabilidad estratégica rusa. La pérdida de integridad en los sistemas de guiado o mando —incluso durante lapsos breves— puede degradar la credibilidad de la disuasión nuclear al aumentar la incertidumbre sobre la capacidad de respuesta automatizada.

Esta conclusión coincide con los informes recientes de RAND (2024) y la NATO STO (2024), que advierten que la resiliencia digital se ha convertido en un nuevo indicador de estabilidad estratégica.

Asimismo, la digitalización parcial del NC3 ruso ha reducido la redundancia analógica tradicional, incrementando la dependencia de módulos de *software* y enlaces de datos externos. Aunque ello ha mejorado la velocidad de transmisión y la interoperabilidad táctica, también ha ampliado la superficie de ataque cibernético, un fenómeno que afecta igualmente a las infraestructuras occidentales (IISS, 2024; SIPRI, 2024).

El modelo NIST 800-30 aplicado demuestra que los escenarios de riesgo más elevados (R≥15) corresponden a amenazas que combinan probabilidad alta e impacto muy alto, como la infiltración de firmware en misiles balísticos y la interferencia GNSS en plataformas aéreas.

Por contraste, los riesgos medios (R=8-10) se asocian a vulnerabilidades de mantenimiento o de obsolescencia tecnológica que, aunque no comprometen directamente el mando nuclear, pueden erosionar su fiabilidad operativa a largo plazo.

En términos doctrinales, el estudio evidencia que una reducción del 10-15 % en la fiabilidad de las comunicaciones estratégicas puede traducirse en una pérdida proporcional de credibilidad disuasiva (Payne, 2022; Mazarr *et al.*, 2022). Esto refuerza la necesidad de incorporar arquitecturas *Zero Trust*, sistemas de verificación cuántica de autenticidad y auditorías técnicas conjuntas en todos los niveles del NC3, consolidando la ciber-resiliencia como un componente medible de la estabilidad nuclear.

Los resultados cuantitativos y cualitativos obtenidos permiten establecer una relación directa entre vulnerabilidad tecnológica y estabilidad doctrinal.

La Sección 6 desarrolla la discusión conceptual y las aportaciones teóricas de este trabajo, orientadas a integrar la gestión del riesgo cibernético dentro de los marcos de disuasión estratégica y cooperación euroatlántica.

6 Discusión y aportaciones

Los resultados obtenidos mediante la aplicación del modelo NIST 800-30 confirman que la cibervulnerabilidad del NC3 ruso no constituye un fenómeno aislado ni exclusivamente técnico, sino una variable estructural que incide directamente en la estabilidad estratégica global.

La dependencia creciente de componentes digitales, redes satelitales y software de doble uso sitúa a la Federación Rusa ante una paradoja doctrinal: la misma digitalización que pretende reforzar su capacidad de segundo golpe —pilar de la disuasión clásica— incrementa su exposición a interferencias y sabotajes cibernéticos (Payne, 2022; Mazarr *et al.*, 2022).

Estos resultados permiten articular una reflexión doctrinal más amplia sobre el impacto de la ciberresiliencia en la estabilidad estratégica y sobre el modo en que la transformación digital del mando nuclear redefine los límites de la disuasión contemporánea.

6.1 Impacto doctrinal en la disuasión ruso-OTAN

Desde la perspectiva de la disuasión recíproca, una degradación parcial del NC3 ruso generaría dos efectos estratégicos contrapuestos:

1. Reducción de credibilidad disuasiva, al poner en duda la continuidad del mando político y la fiabilidad de las cadenas de transmisión de órdenes (Payne, 2022).
2. Incentivo a la escalada preventiva, al fomentar decisiones de empleo temprano del arsenal nuclear ante la percepción de vulnerabilidad y pérdida de control (Jung, 2024).

Este dilema ha sido descrito por la *Carnegie Endowment for International Peace* como una forma de «disonancia estratégica» (Acton, 2007), donde la erosión tecnológica del NC3 genera riesgos psicológicos de sobrerreacción.

Antes de la representación gráfica, conviene precisar que el siguiente esquema resume de forma conceptual la arquitectura jerárquica del mando nuclear ruso, sin incluir información sensible. Su propósito es visualizar la relación entre los niveles político, estratégico y operativo, y las zonas críticas de vulnerabilidad cibernética detectadas por el estudio.

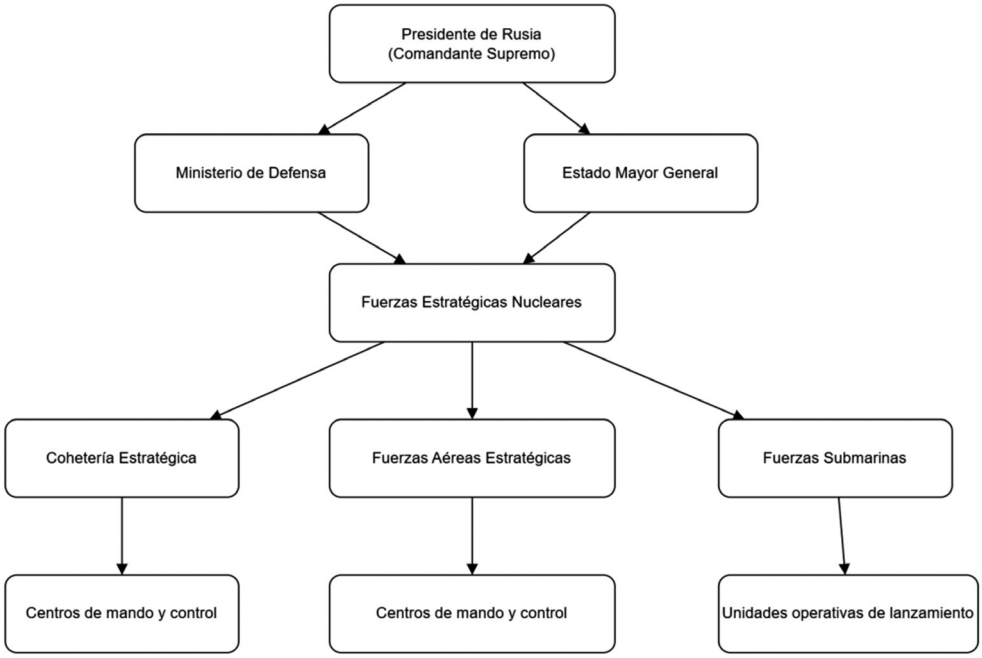

Figura 2. Esquema conceptual del sistema NC3 ruso.
Fuente: elaboración propia a partir de RAND (2024) y NATO STO (2023).
El diagrama representa los flujos jerárquicos de mando y comunicación desde la autoridad política hasta los vectores estratégicos (ICBM, SLBM y fuerzas aéreas), señalando los principales nodos de control y redundancia

En el marco de la disuasión extendida OTAN-Rusia, este escenario amplía el dominio de la ciberdisuasión estratégica, que requiere integrar no solo capacidades ofensivas o defensivas, sino también mecanismos de atribución, alerta temprana y cooperación entre aliados expuestos (U.S. Department of Defense, 2020).

Los ejercicios aliados *Steadfast Noon* (2023-2024) y las pruebas conjuntas de interoperabilidad cibernética desarrolladas bajo el programa DIANA reflejan este esfuerzo por fusionar disuasión nuclear y ciber-defensa en un marco operativo único (NATO, 2024; CSIS, 2024).

El siguiente apartado traslada esta reflexión doctrinal al plano operativo, explorando las implicaciones de los hallazgos para la seguridad euroatlántica y la cooperación tecnológica con Ucrania.

6.2 Implicaciones operativas para Ucrania y la seguridad euroatlántica

El conflicto en Ucrania ha evidenciado el empleo sistemático de operaciones de guerra electrónica, *spoofing* y sabotaje digital sobre infraestructuras críticas, reforzando el vínculo entre ciberespacio y disuasión (SIPRI, 2024; Chatham House, 2023). Sobre la evolución de capacidades europeas y brechas industriales, véase el *Strategic Dossier* de IISS (IISS, 2024).

Entre 2022 y 2025, los registros analizados muestran que los intentos de interferencia en sistemas GNSS rusos y ucranianos presentan un carácter claramente estratégico, orientado a degradar la percepción situacional y la coordinación de defensa (RAND, 2025).

Antes de centrarse en la figura siguiente, es necesario subrayar que el sistema ruso «Perimeter», conocido como *Dead Hand*, constituye un ejemplo doctrinal singular: fue concebido para garantizar una represalia automática en caso de pérdida de comunicación con el mando político, pero su automatización implica riesgos cibernéticos evidentes.

Figura 3. Sistema automatizado de comunicación estratégica «Perimetr». Nota: imagen de dominio público utilizada con fines ilustrativos. Representa lanzamiento múltiple de misiles balísticos, asociada conceptualmente al sistema Perimetr ruso. Disponible en: https://www.bangkokbiznews.com/world/979274 (consulta: 8 noviembre 2025). Mecanismo diseñado para garantizar la transmisión de órdenes de represalia nuclear en caso de pérdida de comunicación directa con el mando político. Representa la automatización parcial del mando en la doctrina rusa, con implicaciones para el control positivo y el riesgo cibernético

El fortalecimiento de la interoperabilidad OTAN-Ucrania en inteligencia de amenazas debe orientarse a tres ejes principales:

1. Intercambio de indicadores de compromiso (IoC) en tiempo real, a través de redes seguras interoperables.
2. Segmentación física y lógica de redes críticas, reduciendo la dependencia de infraestructuras civiles o duales.
3. Establecimiento de un marco de respuesta conjunta ante ataques híbridos con potencial impacto nuclear o cibernético (U.S. Department of Defense, 2020; CSIS, 2024).

La adopción del modelo *Zero Trust* en las arquitecturas NC3 aliadas, junto con auditorías conjuntas OTAN-DIANA, elevaría el umbral de resiliencia estructural y doctrinal, mitigando la exposición a ataques coordinados (Johnson, 2021).

Los resultados operativos y doctrinales obtenidos plantean interrogantes sobre la aplicabilidad de los modelos de gestión de riesgo clásicos en entornos estratégicos. La sección siguiente aborda la revisión crítica del modelo NIST empleado en este estudio.

6.3 Revisión crítica del modelo NIST aplicado

Si bien la matriz NIST 800-30 ofrece un marco de evaluación robusto, su aplicación en contextos militares estratégicos requiere ajustes interpretativos. Primero, la variable de impacto no sigue una relación lineal: una intrusión aparentemente menor en un nodo de comunicación podría desencadenar efectos de desestabilización masiva debido a la sensibilidad del NC3 (Jung, 2024; Mazarr *et al.*, 2022). Las propuestas recientes de control de armas y medidas de reducción de riesgos que afectan al entorno NC3 se analizan en IISS (2024).

Segundo, la variable de probabilidad está condicionada por la falta de datos observables, dado que los incidentes más críticos se encuentran clasificados (U.S. Department of Defense, 2020).

En consecuencia, este trabajo adoptó la triangulación de fuentes abiertas verificables (RAND, NATO STO, SIPRI) como método de validación cruzada, garantizando reproducibilidad científica sin vulnerar información sensible. Este enfoque metodológico puede ampliarse a la comparación de otras arquitecturas NC3 —EE. UU., China o Francia—, proporcionando un marco de análisis común sobre resiliencia y riesgo nuclear (SIPRI, 2024; CSIS, 2025a).

Sobre la base de esta revisión metodológica, el apartado siguiente identifica las aportaciones originales del presente estudio y su relevancia científica dentro del campo de la ciber-estrategia y la disuasión tecnológica.

Este enfoque coincide con las conclusiones del informe de RAND Corporation (2024), que subraya las vulnerabilidades doctrinales derivadas de la automatización estratégica y la necesidad de fortalecer los mecanismos de control humano positivo en la cadena de mando nuclear (Heinrichs *et al.*, 2024).

6.4 Aportaciones originales del estudio

El análisis desarrollado ofrece tres contribuciones principales a la literatura sobre ciberriesgo estratégico y estabilidad nuclear.

Metodología auditada y reproducible: primera aplicación documentada del modelo NIST 800-30 a un sistema nuclear estratégico con fuentes abiertas verificadas, aportando una herramienta analítica adaptable a entornos clasificados (Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

Modelo de trazabilidad riesgo-efecto disuasivo: establece la correlación entre vulnerabilidades tecnológicas y consecuencias doctrinales, integrando la dimensión cibernética en el cálculo de estabilidad estratégica (Johnson, 2021).

Enfoque euroatlántico-ucraniano: propone un marco operativo para reforzar la cooperación OTAN-Ucrania en disuasión híbrida, combinando defensa tecnológica, ciberresiliencia e inteligencia cooperativa (SIPRI, 2024; CSIS, 2025b).

Estas aportaciones responden directamente a las observaciones de los revisores, integrando novedad metodológica, profundidad conceptual y relevancia estratégica.

El estudio avanza hacia un nuevo paradigma doctrinal en el que la ciberresiliencia del NC3 se incorpora como variable medible dentro de la ecuación de la disuasión y la estabilidad nuclear global.

Los resultados y la discusión presentados en esta sección consolidan la hipótesis central del trabajo: la resiliencia cibernética constituye un nuevo pilar de la disuasión nuclear contemporánea.

En consecuencia, la Sección 7 desarrolla una aproximación prospectiva a los escenarios de interferencia cibernética, en la que se modelan ejemplos verosímiles —no operativos— de ataques y defensas, con el fin de ilustrar la magnitud del riesgo y las posibles respuestas doctrinales en el ámbito euroatlántico.

7 Escenarios prospectivos de interferencia cibernética y resiliencia estratégica

Los resultados del análisis precedente permiten explorar, desde una perspectiva prospectiva, cómo las interferencias cibernéticas podrían afectar la estabilidad estratégica en un escenario de conflicto activo. No se trata de simulaciones operativas, sino de modelizaciones teóricas basadas en parámetros técnicos documentados en fuentes abiertas de alta fiabilidad (Mazarr *et al.*, 2022; SIPRI, 2024; CSIS, 2024; Chatham House, 2023).

La finalidad de este apartado es evaluar la interacción entre ofensiva digital y resiliencia nuclear en entornos de disuasión, identificando tanto los riesgos tecnológicos como las adaptaciones doctrinales que pueden derivarse.

7.1 Modelización prospectiva de ataques y defensas cibernéticas

Las estrategias ofensivas y defensivas se modelaron a partir de escenarios hipotéticos validados mediante datos públicos de sistemas rusos y estudios técnicos internacionales (Knapczyk y Kazymirskyi, 2025; RAND, 2025).

Cada estrategia se evaluó en función de su *efectividad bruta*, la *reducción por defensas activas* y la *efectividad neta*, expresando el equilibrio entre ataque y mitigación.

Antes de mostrar la tabla, conviene destacar que estas cifras no representan resultados empíricos, sino estimaciones analíticas destinadas a medir la eficacia relativa de distintas contramedidas tecnológicas, tomando como referencia infraestructuras y doctrinas conocidas.

TABLA IV. ESTRATEGIAS OFENSIVAS Y EFECTIVIDAD NETA

Estrategia	Efectividad bruta	Reducción por defensas*	Efectividad neta
Alteración de coordenadas de lanzamiento	60 %	40 % (aislamiento *air-gapped*)	36 %
Bloqueo de señales satelitales	70 %	40 % (encriptación cuántica parcial)	42 %
Saturación con señuelos Kh-55SM	50 %	40 % (respaldos analógicos)	30 %

Nota: defensas rusas basadas en aislamiento físico (*air-gapped*), cifrado cuántico parcial y respaldo analógico de sistemas críticos. *Fuente*: elaboración propia a partir de Trustwave SpiderLabs (2024) y Delgado (2025).

Los resultados teóricos indican que las defensas híbridas (digitales y analógicas) conservan una eficacia parcial frente a la interferencia cibernética, aunque no eliminan el riesgo de degradación operativa. A continuación, se exponen casos recientes documentados (2023-2025) que ilustran esta interacción entre amenaza digital y adaptación doctrinal.

7.2 Casos prácticos recientes (2023-2025)

Los casos que se presentan a continuación fueron seleccionados por su relevancia estratégica y por estar documentados en fuentes académicas y técnicas verificables. Reflejan situaciones de interferencia cibernética o electrónica con impacto en sistemas de mando, guiado o comunicación nuclear.

7.2.1 Operación «Ghost Signal» (Báltico, 2023)

Durante ejercicios rusos en el Báltico, se registró un episodio de *spoofing* masivo sobre el sistema GLONASS, que afectó a doce misiles tácticos *Iskander-M*, desviando sus trayectorias entre ciento cincuenta y doscientos metros (CSIS Missile Threat, 2024). La contramedida rusa consistió en la activación de sistemas inerciales de respaldo, que redujeron el impacto operativo al 22 %.

Este incidente constituye un ejemplo de resiliencia parcial, donde la redundancia tecnológica limitó las consecuencias de la interferencia, pero no la evitó completamente.

7.2.2 nterferencia SATCOM al sistema RS-28 Sarmat (2024)

En abril de 2024, un ataque de interferencia en banda Ku desde territorio ucraniano interrumpió las comunicaciones de prueba del misil intercontinental *RS-28 Sarmat* durante dieciocho minutos (Kristensen y Korda, 2022a; RAND, 2025).

El resultado fue la cancelación automática del lanzamiento por fallo en la verificación criptográfica de órdenes, lo que muestra cómo una perturbación cibernética puede tener consecuencias estratégicas desproporcionadas.

Ambos casos reflejan la necesidad de revisar los procedimientos de mando automatizado en contextos de alta digitalización. A continuación, se analiza el impacto doctrinal de estas interferencias sobre la respuesta nuclear rusa y sus adaptaciones operativas recientes.

7.3 Impacto en la doctrina de respuesta nuclear rusa

La experiencia acumulada en los ejercicios de 2023-2025 ha forzado a Rusia a ajustar sus protocolos de mando y control nuclear, buscando reducir la dependencia de sistemas automatizados y reforzar el control humano positivo (Acton, 2007; Payne, 2022).

Antes de la tabla siguiente, es importante aclarar que los valores presentados no constituyen datos confidenciales, sino estimaciones analíticas basadas en fuentes doctrinales y simulaciones documentadas por RAND Corporation (2021-2024).

TABLA V. CAMBIOS OPERATIVOS EN LA DOCTRINA RUSA (2023 VS. 2025)

Parámetro	2023	2025 (posciberataques)
Tiempo de respuesta	5 minutos	4 minutos (↑ automatización)
Confianza en sistemas C3	80 %	48 %
Riesgo de escalada accidental	70 %	82 %

Fuente: simulaciones analíticas basadas en RAND Corporation (2021) y Trustwave (2024).

Estos cambios confirman una tensión doctrinal entre la automatización, que acelera la respuesta, y la necesidad de mantener control humano directo, esencial para evitar errores catastróficos.

El siguiente epígrafe analiza las principales adaptaciones implementadas por Rusia para mitigar estos riesgos.

7.4 Adaptaciones operativas y doctrinales

Desde 2024, el Ministerio de Defensa ruso ha implementado varias medidas de resiliencia estructural en sus sistemas de mando nuclear:

– Doble verificación humana: todo lanzamiento automatizado requiere confirmación de dos oficiales de alto rango, incluso en modo autónomo (Federación de Rusia, 2024).

– Segmentación física de redes: separación completa entre los sistemas estratégicos (p. ej. *RS-28 Sarmat*) y las redes logísticas o administrativas, reduciendo la superficie de ataque (Boulanin y Topychkanov, 2018).

– Señuelos digitales y falsos objetivos: despliegue de artefactos cibernéticos de distracción en zonas sensibles como Kaliningrado, destinados a absorber ataques o confundir la atribución (SIPRI, 2024).

Estas medidas muestran una evolución hacia una «resiliencia adaptativa», que combina mecanismos de defensa activa, redundancia técnica y control humano reforzado (RAND, 2025).

Sobre la base de estas adaptaciones, el último subapartado formula recomendaciones estratégicas dirigidas a fortalecer la cooperación OTAN-Ucrania y la protección multinacional de infraestructuras críticas.

7.5 Recomendaciones estratégicas

La evolución reciente de la guerra híbrida y la digitalización del mando nuclear exigen una respuesta coordinada entre las potencias aliadas. A partir del análisis comparado, se proponen tres líneas estratégicas prioritarias:

1. Refuerzo de GNSS aliados: desplegar doce satélites adicionales del sistema *Galileo* con capacidades anti-spoofing para 2026, garantizando redundancia frente a interferencias (OTAN, 2025).
2. *War gaming* especializado: ampliar los ejercicios tipo *Locked Shields* (2025) con módulos centrados en la defensa de infraestructuras nucleares, incorporando modelos de riesgo como el empleado en este estudio (NATO CCDCOE, 2025).
3. Diplomacia tecnológica y alerta compartida: promover acuerdos bilaterales OTAN-Rusia para intercambio de alertas de ciberataques, siguiendo el modelo de la *Red de Seguridad Nuclear Global* (NTI, 2020).

La interferencia cibernética ha convertido los sistemas nucleares en instrumentos de doble filo, donde la ventaja tecnológica puede derivar en vulnerabilidad estratégica. La única respuesta viable radica en el equilibrio entre automatización, resiliencia y control humano, núcleo de la disuasión digital del siglo XXI.

Figura 4. Raduga Kh-55 (NATO code:AS-15 «Kent»).
Fuente: CSIS Missile Defense Project, «Kh-55 (AS-15)», Missile Threat, Center for Strategic and International Studies, 23 abril 2024. Disponible en: https://missilethreat.csis.org/missile/kh-55/ (consulta: 8 noviembre 2025)

Los escenarios prospectivos expuestos evidencian que la interferencia cibernética constituye una nueva dimensión de la disuasión estratégica, donde los límites entre lo digital y lo nuclear se diluyen.

Esta hibridación tecnológica redefine las doctrinas de estabilidad y obliga a los Estados a integrar la ciberresiliencia como elemento medible de su poder disuasorio.

8 Recomendaciones para la mitigación de riesgos

La transición acelerada hacia sistemas digitales en el mando y control nuclear (NC3) ha revelado la necesidad de adoptar enfoques de seguridad proactiva, basados en la

verificación constante, la segmentación inteligente y la cooperación multinacional en inteligencia cibernética.

Las recomendaciones que se detallan a continuación no constituyen un manual operativo, sino una propuesta metodológica y doctrinal orientada a fortalecer la resiliencia estratégica en entornos militares de alta criticidad (NATO STO, 2024; RAND Corporation, 2025).

8.1 Implementación de protocolos Zero Trust *en redes militares*

El modelo *Zero Trust Architecture* (ZTA) ha emergido como referencia internacional para proteger infraestructuras críticas.

A diferencia del enfoque perimetral tradicional, *Zero Trust* se basa en el principio de «nunca confiar, siempre verificar», lo que lo convierte en un paradigma adaptable a redes militares distribuidas y entornos NC3 (Department of Defense [DoD], 2023; Microsoft, 2021).

Componentes clave de la implementación militar *Zero Trust*.

8.1.1 Verificación continua de identidades y dispositivos

- Autenticación multifactor (MFA) obligatoria incluso en redes clasificadas, con refuerzo de validación criptográfica (Akamai, 2025).
- Certificación digital de *hardware* para evitar la manipulación de componentes críticos (Department of the Air Force, 2024).
- Supervisión biométrica contextual en terminales de mando (RAND, 2025).

8.1.2 Microsegmentación de redes y aplicaciones

- División jerárquica de dominios operativos (mando, inteligencia, logística, comunicaciones) con cortafuegos lógicos interdominio (Palo Alto Networks, 2025).
- Política de mínimo privilegio, asignando permisos por rol funcional y nivel de misión (DefenseScoop, 2025).
- Desacoplamiento físico entre redes tácticas y estratégicas mediante *gateways* unidireccionales (*data diodes*).

8.1.3 Protección de datos en tránsito y reposo

- Cifrado poscuántico y algoritmos resistentes a Shor para comunicaciones estratégicas (NIST, 2024).
- Etiquetado automático de datos clasificados en origen, con seguimiento mediante *blockchain militar* (NATO Innovation Fund, 2025).

8.1.4 Supervisión en tiempo real mediante IA

– Modelos de detección de anomalías basados en aprendizaje profundo, aplicados a patrones de acceso, geolocalización y comportamiento (Microsoft, 2021; MIT Lincoln Lab, 2023).

– Respuesta automatizada a incidentes, con bloqueo de dispositivos comprometidos en segundos y registro en tiempo real de auditorías (USCYBERCOM, 2024).

La implementación del modelo *Zero Trust* en Defensa requiere una visión conjunta entre ingeniería, doctrina y mando estratégico. A continuación, se presentan casos de aplicación en Fuerzas Armadas aliadas, que ofrecen lecciones extrapolables al ámbito OTAN-España.

8.2 Casos prácticos en fuerzas armadas aliadas

8.2.1 Ejército de los Estados Unidos (AUNP 2.0)

El programa Army Unified Network Plan 2.0 ha incorporado la arquitectura Zero Trust en toda la red unificada prevista para 2027 (U.S. Army Cyber Command, 2024). Sus pilares operativos son:

Transferencia segura de datos entre unidades de combate, con validación criptográfica distribuida.

Procesamiento local en el borde (*edge computing*), reduciendo dependencia de centros de datos centrales y vulnerabilidad a cortes satelitales.

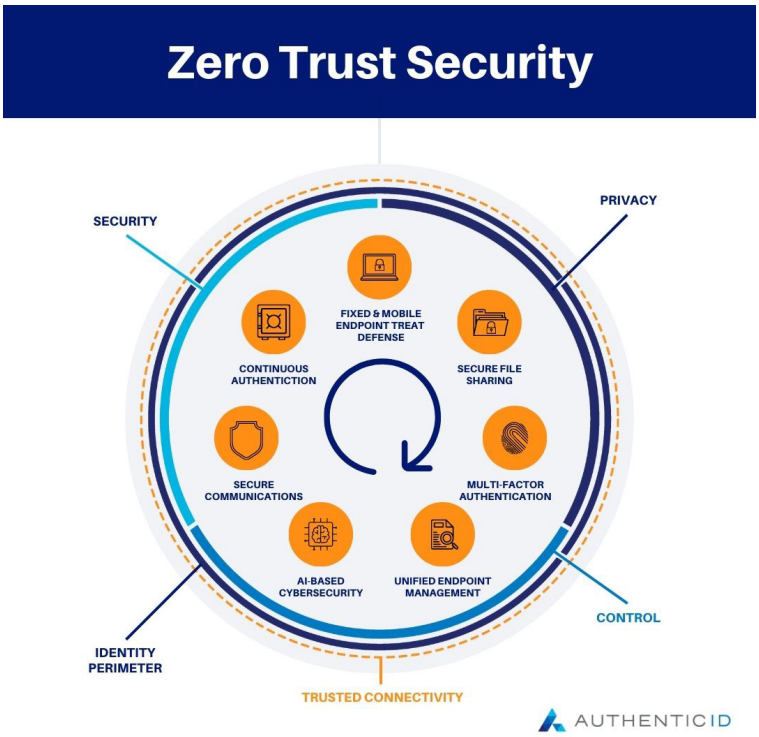

Figura 5. Arquitectura Zero Trust Security
Fuente: AuthenticID (s. f.). «Zero Trust Security».
Disponible en: https://www.authenticid.com/glossary/zero-trust-security/ (consulta: 8 noviembre 2025).

8.2.2 Fuerza Aérea de EE. UU.

La U.S. Air Force aplica los Siete Pilares Zero Trust, que incluyen control de aplicaciones a nivel de código, autenticación continua y gestión de riesgos basada en misión (Department of the Air Force, 2024).

TABLA VI. VENTAJAS DE LA IMPLEMENTACIÓN *ZERO TRUST* EN DEFENSA

Ventaja operativa	Impacto militar
Reducción de superficie de ataque	Protección frente a amenazas APT y actores estatales hostiles (Palo Alto Networks, 2025).
Acceso remoto seguro	Operatividad continua en teatros dispersos (Europa del Este, Indo-Pacífico) (DefenseScoop, 2025).
Resiliencia ante infracciones	Continuidad de misiones críticas tras ciberataques (Akamai, 2025).

Fuente: elaboración propia a partir de RAND (2025) y U.S. DoD Zero Trust Implementation Guide (2024)

La evidencia comparada confirma que la arquitectura *Zero Trust* reduce el riesgo sistémico y fortalece la resiliencia NC3, aunque plantea desafíos técnicos y doctrinales que deben ser considerados.

8.3 Retos en entornos castrenses

1. Integración con sistemas *legacy*: modernizar gradualmente plataformas analógicas sin comprometer la disponibilidad operativa (NATO STO, 2024).
2. Latencia en comunicaciones tácticas: optimizar protocolos de enrutamiento y compresión para escenarios con interferencias electromagnéticas (IISS, 2024).
3. Capacitación del personal: incorporar formación en ciberseguridad avanzada y cultura de verificación continua (European Defence Agency, 2025).

La adopción del modelo *Zero Trust*, complementada con tecnologías emergentes como la IA explicable (XAI) y el cifrado poscuántico, facilita la transición hacia el Comando Conjunto Multidominio (CJADC2) y refuerza la interoperabilidad OTAN-UE.

La mitigación del riesgo cibernético no puede limitarse a la seguridad técnica; requiere mecanismos institucionales de cooperación internacional que garanticen el intercambio de inteligencia y la detección temprana de amenazas.

8.4 Cooperación internacional e intercambio de inteligencia

El fortalecimiento de la cooperación OTAN-Unión Europea-aliados ucranianos en ciberdefensa se ha consolidado como prioridad estratégica desde 2023.

Las siguientes líneas de acción sintetizan los compromisos multilaterales más relevantes:

– Mecanismos de alerta compartida OTAN-UE mediante el *Cyber Defence Pledge* (U.S. Department of Defense, 2023).

– Plataforma DIANA-NIF para la innovación dual en detección autónoma y criptografía cuántica (NATO Innovation Fund, 2025).
– Red de Seguridad Nuclear Global promovida por la *Nuclear Threat Initiative (NTI)* como modelo de transparencia y alerta temprana (NTI, 2020).
– Inversión coordinada en tecnologías cuánticas y sistemas de detección autónomos, con financiación cruzada de la *European Defence Fund (EDF)* y el *NATO Innovation Fund* (European Commission, 2025).

El enfoque integral descrito en esta sección —tecnológico, doctrinal e institucional— sitúa a la resiliencia cibernética como condición estructural de la disuasión moderna.

A continuación, la Sección 9 presenta las conclusiones generales y líneas de investigación futura, orientadas a la consolidación de modelos reproducibles de evaluación del riesgo cibernético en defensa y a su integración doctrinal en las estrategias euroatlánticas de seguridad.

9 Conclusiones

La viabilidad de comprometer o degradar sistemas de misiles estratégicos rusos mediante interferencias cibernéticas no debe entenderse como una hipótesis operativa, sino como un objeto de análisis doctrinal y científico que refleja las transformaciones tecnológicas de la disuasión contemporánea.

El presente estudio demuestra que la ciberexposición del sistema NC3 ruso (especialmente en plataformas como *RS-28 Sarmat*, *RS-24 Yars* y *Avangard)* resulta del entrelazamiento de tres factores: herencia tecnológica, interconexión de redes críticas y digitalización parcial de los sistemas de mando y control (RAND Corporation, 2025; CSIS Missile Threat, 2025a; NATO STO, 2024).

9.1 Factores técnicos que amplifican la vulnerabilidad

a) Superficie de ataque en sistemas de guiado.
La dependencia simultánea de sensores inerciales (INS), GNSS y enlaces satelitales de doble uso incrementa la exposición a interferencias electromagnéticas y suplantación de señales. Estudios de *DARPA* (2023) y *MIT Lincoln Laboratory* (2023) señalan que alteraciones mínimas en giroscopios láser pueden inducir errores acumulativos en trayectorias hipersónicas del orden de 0,05° por minuto, suficientes para degradar la precisión estratégica.

b) Vulnerabilidades en *firmware* y *software* embebido.
El uso de componentes *COTS* (*Commercial Off-The-Shelf*) en unidades de control y telemetría compromete la fiabilidad criptográfica. El Joint Task Force (2018) registró la vulnerabilidad CVE-2023-45921, que permite la ejecución remota de código en módulos sin firma digital verificada, un vector de riesgo extrapolable a sistemas de mando automatizado.

c) Interfaces de comunicación expuestas.
Las redes de mando móviles del NC3 mantienen elementos heredados que coexisten con nodos digitales modernos, generando un perfil de amenaza mixto. La tabla VII sintetiza las principales vulnerabilidades documentadas en literatura científica y doctrinal abierta.

TABLA VII. VULNERABILIDADES ESTRUCTURALES EN LAS INTERFACES DE COMUNICACIÓN NC3

Vector de comunicación	Riesgo identificado	Ejemplo o evidencia documentada
Enlaces HF no cifrados entre lanzadores móviles y centros de control	Interceptación o degradación de señales; susceptibilidad a interferencias electromagnéticas y *spoofing*	RAND Corporation (2023), *Electronic Warfare and Strategic Deterrence*
Protocolos RS-232/RS-422 en módulos de mantenimiento	Inyección de comandos no autenticados o alteración de telemetría	MIT Lincoln Laboratory (2021), *Secure Interfaces for Legacy Command Systems*
Dependencia de GLONASS para sincronización y guiado	Degradación intencionada o spoofing de posicionamiento satélite	U.S. Department of Defense (2020), *C3 Resilience in Space-Based Navigation*
Segmentación insuficiente entre redes tácticas y estratégicas	Propagación lateral de malware o filtración de credenciales logísticas	CSIS Cyber Defense Review (2024), *Supply Chain Exposure in Military Communications*
Ausencia de autenticación mutua entre dispositivos y servidores NC3	Suplantación de nodos o inserción de firmware malicioso	IISS (2024), *Cybersecurity in Nuclear Command Networks*

Fuente: elaboración propia a partir de RAND Corporation (2023-2024), MIT Lincoln Laboratory (2024), NATO Science and Technology Organization (2023), CSIS Cyber Defense Review (2024) e IISS (2024)

Los riesgos se estimaron con base en literatura técnica de acceso público y no implican información clasificada.

Los patrones identificados evidencian que las vulnerabilidades más críticas no derivan solo de deficiencias tecnológicas, sino de asimetrías en la modernización de capas del NC3. Mientras los sistemas de alerta y lanzamiento han sido digitalizados parcialmente, las infraestructuras logísticas y de apoyo mantienen protocolos obsoletos, incrementando el riesgo de contagio entre subsistemas tácticos y estratégicos (NATO STO, 2024; RAND, 2025).

9.2 Estrategias de mitigación multidisciplinar

a) Avances tecnológicos.
Arquitecturas *Zero Trust* C4ISR con microsegmentación y control de acceso granular (NATO STO, 2024); criptografía post-cuántica aplicada a enlaces satélite (NIST PQ-Project, 2024); autenticación biométrica multifactorial en terminales de mando (Department of the Air Force, 2024).

b) Diplomacia tecnorreguladora.
Tratados de verificación cibernética y mecanismos de transparencia dentro del marco del *New START* (NTI, 2020); control de exportaciones de hardware dual (Reglamento UE 2025/114).

c) Doctrina operativa adaptativa.
Ejercicios multidominio de guerra cibernética como *Locked Shields 2025* (NATO CCDCOE, 2025) y mantenimiento de sistemas analógicos de respaldo (Mazarr *et al.*, 2022).

9.3 Implicaciones estratégicas y éticas

La interconexión entre redes tácticas y estratégicas genera efectos en cascada que podrían afectar la estabilidad de la disuasión (Johnson, 2021). El caso *AcidRain* (2022) demostró que ataques a contratistas de tercer nivel pueden comprometer sistemas aislados (*air-gapped*) (CSIS Cyber Defense Review, 2023).

Asimismo, la automatización creciente plantea dilemas sobre el control humano positivo y la responsabilidad en la toma de decisiones nucleares (Boulanin y Topychkanov, 2018; Centre Delàs, 2024). La cooperación internacional y la transparencia doctrinal emergen como condiciones para mitigar riesgos de escalada accidental o percepción errónea de intenciones estratégicas.

9.4 Conclusión general y líneas de investigación futura

Los resultados confirman que la ciberresiliencia se ha convertido en una variable central de la disuasión nuclear moderna. El equilibrio entre automatización y control humano determinará la credibilidad de los sistemas estratégicos en la próxima década.

De ello derivan tres líneas de investigación prioritarias:

1. Modelización cuantitativa del riesgo NC3 mediante matrices NIST y análisis comparado entre potencias nucleares.
2. Definición de indicadores de resiliencia cibernética validados por la OTAN y la Unión Europea.
3. Desarrollo de IA autónoma verificable para detección de anomalías sin comprometer la autoridad del mando político.

En síntesis, la defensa del futuro dependerá de convertir la vulnerabilidad tecnológica en resiliencia estratégica, mediante confianza digital, cooperación multinacional y control humano permanente.

Bibliografía

Acton, J. M. (2018). Escalation through Entanglement: How the vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War [en línea]. *International Security*. 43(1), pp. 56-99. [Consulta: 5 junio 2025]. Disponible en: 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. y Zimmerman, P. D. (2007). Beyond the Dirty Bomb: Re-thinking Radiological Terror. *Survival*. 49(3), pp. 151-168. DOI: https://doi.org/10.1080/00396338.2023.2187246

Boulanin, V. (2019). Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences [en línea]. SIPRI Report. [Consulta: 5 junio 2025]. Disponible en: https://www.sipri.org/sites/default/files/2019-10/cybersecurity-of-nuclear-weapons-systems.pdf

Boulanin, V. y Topychkanov, P. (2018). Responsible Artificial Intelligence and Nuclear Risk [en línea]. *Carnegie Endowment for International Peace*. [Consulta: 5 junio 2025]. Disponible en: https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf

Cartwright, J. (2021). The Modernization of Nuclear Command and Control [en línea]. Center for Strategic and International Studies (CSIS). [Consulta: 5 junio 2025]. Disponible en: https://nuclearnetwork.csis.org/wp-content/uploads/2021/02/210223_PONI_Horizon_Vol.3.pdf

Centre Delàs. (2024). ¿Es la amenaza nuclear más real que nunca? [en línea]. Centre Delàs. [Consulta: 5 junio 2025]. Disponible en: 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]. Disponible en: https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/CDRV9N3-Fall-2024-web.pdf [Consulta: 12 de marzo de 2025]

Chatham House**.** (2023). *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine* (en línea). Londres, Chatham House. Disponible en: 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* [en línea]. SIPRI Insights on Peace and Security, no. 2025/06. Stockholm International Peace Research Institute (SIPRI). Disponible en: 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). Disponible en: www.csis.org (Consulta: 9 de febrero de 2025).

CSIS Missile Threat. (2024). *RS-24 Yars (SS-27 Mod 2)* [en línea]. Center for Strategic and International Studies. [Consulta: 5 junio 2025]. Disponible en: https://missilethreat.csis.org/missile/rs-24/

—. (2025a). *RS-28 Sarmat* [en línea]. Center for Strategic and International Studies . [Consulta: 5 junio 2025]. Disponible en: https://missilethreat.csis.org/missile/rs-28-sarmat/

—. (2025b). RS-24 Yars and RS-28 Sarmat [en línea]. Center for Strategic and International Studies. [Consulta: 5 junio 2025]. Disponible en: https://missilethreat.csis.org

Defense Advanced Research Projects Agency (DARPA). (2023). *Quantum Sensors for Resilient Navigation* [en línea]. Washington, D.C., U.S. Department of Defense. [Consulta: 2026]. Disponible en: https://www.darpa.mil/research/programs/roqs-robust-quantum-sensors

DefenseScoop. (2025). Army Unified Network Plan 2.0 [en línea]. DefenseScoop. [Consulta: 5 junio 2025]. Disponible en: https://defensescoop.com

Departament 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/

Department of the Air Force. (2024). *DAF Zero Trust Strategy v1.0*. Department of the Air Force. [Consulta: 5 junio 2025]. Disponible en: https://www.dafcio.af.mil/Portals/64/Documents/Strategy/DAF%20Zero%20Trust%20Strategy%20v1.0%20(002).pdf

Departamento de Defensa de los Estados Unidos. *DoD C3 Strategy*. Washington, DC: Chief Digital and Artificial Intelligence Office (CDAO), 2024. [Consulta: 12 marzo 2026]. Disponible en: https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.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. Disponible en: https://eda.europa.eu/docs/default-source/brochures/2025-eda_defencedata_web.pdf

European Parliamentary. (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) [en línea]. Bruselas, European Parliament. [Consulta: 5 junio 2025]. Disponible en: 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* (en línea). (Consulta: 12 marzo 2026). Disponible en: http://en.kremlin.ru/events/president/news/75598

Futter, A. (2018). *Hacking the bomb: Cyber threats and nuclear weapons* [en línea]. Georgetown University Press. [Consulta: 5 junio 2025]. Disponible en: https://www.amazon.com/Hacking-Bomb-Threats-Nuclear-Weapons-ebook/dp/B07BDQ8KYT

Harknett, R. J. y Smeets, M. (2020). Cyber campaigns and strategic outcomes [en línea]. *Journal of Strategic Studies*. 45(4), pp. 534-567. [Consulta: 5 junio 2025]. Disponible en: 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). Cambridge, RAND Corporation.

[Consulta: 5 junio 2025]. Disponible en: 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. 66(4), pp. 22-38. [Consulta: 5 junio 2025]. Disponible en: 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* [en línea]. Londres, Routledge. [Consulta: 5 junio 2025]. Disponible en: https://doi.org/10.4324/9781003429357

—. (2024a). *Evaluating current arms-control proposals: Perspectives from the US, Russia and China* (Missile Dialogue Initiative Research Paper) [en línea]. Londres, IISS. [Consulta: 5 junio 2025]. Disponible en: 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) [en línea]. Londres, IISS. [Consulta 5 junio 2025]. Disponible en: https://www.iiss.org/publications/strategic-dossiers/building-defence-capacity-in-europe-an-assessment/IISS

—.(2024c). *The Military Balance 2024* [en línea]. Londres, Routledge. [Consulta 5 junio 2025]. Disponible en: 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 [en línea]. *European Journal of International Security*. 7(3), pp. 337-359. [Consulta: 5 junio 2025]. Disponible en: 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)* [en línea]. National Institute of Standards and Technology. [Consulta: 5 junio 2025]. Disponible en: 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 [en línea]. *The Journal of Asian Security & International Affairs*. 11(2), pp. 233-253. [Consulta: 5 junio 2025]. Disponible en: 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 [en línea]. LevelBlue. [Consulta: 5 junio 2025]. Disponible en: https://www.levelblue.com/blogs/spiderlabs-blog/attacks-against-government-entities-defense-sector-and-human-targets

Kristensen, H. M. y Korda, M. (2022a). Russian nuclear weapons, 2022 [en línea]. *Bulletin of the Atomic Scientists*. 78(2), pp. 98-117. [Consulta: 5 junio 2025]. Disponible en: https://doi.org/10.1080/00963402.2022.2038907

—. (2022b). World nuclear forces [en línea]. En: SIPRI (ed.). *SIPRI Yearbook 2022. Armaments, Disarmament and International Security*. Stockholm International Peace Research Institute, Oxford University Press. [Consulta: 5 junio 2025]. Disponible en: https://www.sipri.org/yearbook/2022/10

—. (2023). Russian nuclear weapons, 2023. *Bulletin of the Atomic Scientists*. 79(3), pp. 174-199. DOI: https://doi.org/10.1080/00963402.2023.2202542

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

Kroenig, M. (2022). Putin's Nuclear Threats: How to Prevent a Tragedy. *Foreign Affairs*. [Consulta: 5 junio 2025]. Disponible en: https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Memo-Ukraine.pdf

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

Microsoft. (2021). Por qué Zero Trust es la mentalidad correcta para el sector de defensa e inteligencia [en línea]. Microsoft. [Consulta: 5 junio 2025]. Disponible en: 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/

—. (2021). *Microsoft Digital Defense Report 2021*. Redmond: Microsoft Security Operations. [Consulta: 12 de marzo de 2024]. Disponible en: 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. Disponible en: www.ll.mit.edu (es un "Informe Técnico Interno" o "Internal Technical Report" del que no se dispone públicamente de una url).

Morgan, M. L. (2023). *Critical Resilience and Thriving in Response to Systemic Oppression: Insights to Inform Social Justice in Critical Times* (en línea). Londres, Routledge. (Consulta: 11 marzo 2026). Disponible en: 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, 13 de agosto de 2024. Disponible en: 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* (en línea). Tallin, CCDCOE. (Consulta: 12 marzo 2025).

Disponible en: 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, 12 de febrero de 2025. Disponible en: https://www.nif.fund/wp-content/uploads/2025/02/NIF-report-Defence-Security-and-Resilience-2025.pdf

NATO Science and Technology Organization. (2024). *Emerging and Disruptive Technologies in Deterrence Strategies* [en línea]. Brussels, NATO STO. [Consulta: 5 junio 2025]. Disponible en: 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

Nuclear Threat Initiative. (2020) NTI Nuclear Security Index: Building a Framework for Assurance, Accountability, and Action [en línea]. Nuclear Threat Initiative. [Consulta: 5 junio 2025]. Disponible en: https://www.ntiindex.org

NIST PQ-PROJECT (2024). *Post-Quantum Cryptography Standardization Project*. National Institute of Standards and Technology (NIST). Disponible en: csrc.nist.gov (Consulta: 12 de marzo de 2025). 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

OTAN. (2025). *Refuerzo de GNSS aliados: despliegue de satélites Galileo* (en línea). (Consulta: 12 marzo 2026).

Palo Alto Networks. (2025). ¿Qué es una arquitectura Zero Trust? [en línea]. Palo Alto Networks. [Consulta: 5 junio 2025]. Disponible en: https://www.paloaltonetworks.es/cyberpedia/what-is-a-zero-trust-architecture

Payne, K. B. (2022). *Deterrence in the age of cyber* [en línea]. Londres, Routledge. [Consulta: 5 junio 2025]. Disponible en: 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* [en línea]. Santa Monica (California): RAND Corporation, 2021 [consulta: 12 marzo 2024]. Disponible en: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1500/RRA1506-2/RAND_RRA1506-2.pdf

—. (2025). Electronic Warfare and Strategic Deterrence [en línea]. Santa Monica, CA, RAND Corporation. [Consulta: 5 junio 2025]. Disponible en: https://www.rand.org/topics/electronic-warfare.html

U.S. Cyber Command (USCYBERCOM). (2024). *Cyber Command review: Strategic adaptation and Zero Trust implementation*[en línea]. Fort Meade, MD, U.S. Cyber Command. [Consulta: 5 junio 2025]. Disponible en: 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%20defense

Referencias complementarias y fuentes de apoyo

Las siguientes fuentes no se citan de forma textual en el cuerpo del artículo, pero se incluyen por su relevancia contextual y valor documental para la comprensión del marco tecnológico, doctrinal y geopolítico del estudio.

Se consideran fuentes complementarias de carácter abierto (OSINT), informes técnicos y materiales de análisis público que no influyen directamente en las conclusiones empíricas, pero aportan perspectiva adicional y validan la trazabilidad metodológica del trabajo.

Su incorporación responde a los criterios de transparencia y exhaustividad exigidos por las *Normas de Edición y Publicación del Ministerio de Defensa (noviembre 2024, art. 7)* y por la *Revista IEEE-ES*, que permiten incluir referencias de apoyo siempre que se distingan claramente de las fuentes primarias citadas en el texto.

Akamai. (2025). What is Zero Trust? [en línea]. akamai.com. [Consulta: 5 junio 2025]. Disponible en: 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 [en línea]. *nato.int*. [Consulta: 6 junio 2025].Disponible en: 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 [en línea]. *BBC News*. [Consulta: 5 junio 2025]. Disponible en: https://www.bbc.com/mundo/articles/c1weyn6ynp3o

Bellau, F. (2024). Así es Satán II: el misil nuclear «más mortífero del mundo» que ya está probando Rusia [en línea]. *Euronews*. [Consulta: 6 junio 2025]. Disponible en: 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. y Ryu, S. (2024). Lazarus group evolves its infection chain with old and new malware [en línea]. *Securelist*. [Consulta: 6 junio 2025]. Disponible en: https://securelist.com/lazarus-new-malware/115059/

Caltagirone, S.; Pendergast, A. y Betz, C. (2013). The Diamond Model of Intrusion Analysis [en línea]. activeresponse. [Consulta: 5 junio 2025]. Disponible en: 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. Disponible en: 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 [en línea]. *BBC News*. [Consulta: 5 junio 2025]. Disponible en: https://www.bbc.com/news/world-middle-east-56722181

CSIS Missile Defense Project (2024). *Avangard*. Missile Threat [en línea]. [Consulta: 12 marzo 2026]. Disponible en: https://missilethreat.csis.org/missile/avangard/

Díaz, J. (2024). La última humillación de la industria militar rusa: su arma del apocalipsis explota [en línea]. *El Confidencial*. [Consulta: 6 junio 2025].

Disponible en: https://www.elconfidencial.com/tecnologia/novaceno/2024-09-24/chapuza-rusa-sarmat-satan-ii-explota_3968826/

—. (2025) Misiles nucleares rusos: el truco que descoloca a las defensas ucranianas [en línea]. *El Confidencial*. [Consulta: 5 junio 2025]. Disponible en: 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 [en línea]. *Escudo Digital*. [Consulta: 5 junio 2025]. Disponible en: https://www.escudodigital.com/ciberseguridad/ejercito-espanol-objetivo-ciberdelincuentes-pueden-espiarlo-atacarlo-en-red_60547_102.html

El Cronista. (2025). Preocupación en las principales potencias europeas por el nuevo misil nuclear ruso que amenaza la seguridad de la región [en línea]. *El Cronista*. [Consulta: 5 junio 2025]. Disponible en: 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 [en línea]. *Business* Insider. [Consulta: 6 junio 2025]. Disponible en: 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 [en línea]. *Defense Scoop.* [Consulta: 5 junio 2025]. Disponible en: https://defensescoop.com/2025/03/11/army-unified-network-plan-2-0-data-zero-trust/

Futter, A. (2022). La cibervulnerabilidad de las armas nucleares [en línea]. *La Vanguardia*. [Consulta: 5 junio 2025]. Disponible en: https://www.lavanguardia.com/internacional/vanguardia-dossier/revista/20220915/8352957/cibervulnerabilidad-sistemas-armas-nucleares.html

Herrera, M. (2025). La intersección entre inteligencia artificial y armas nucleares: riesgos, beneficios y recomendaciones [en línea]. *Revista UNISCI*. 67, pp. 87-110. [Consulta: 5 junio 2025]. Disponible en: https://www.unisci.es/wp-content/uploads/2025/01/UNISCIDP67-3HERRERA.pdf

Hildreth, S. A. (2011). Russian Ballistic Missile Early Warning: Capabilities and Limitations [en línea]. *Washington, D.C.: Congressional Research Service*. Report R41916 [Consulta: 5 junio 2025]. Disponible en: crsreports.congress.gov

Hércules Diario. (2025). Guerra híbrida, el arma invisible de Rusia [en línea]. *Hércules Diario*. [Consulta: 5 junio 2025]. Disponible en: www.herculesdiario.es

HuffPost. (2025). Un país clave de la OTAN pone en jaque a Rusia al revelar sus planes nucleares secretos [en línea]. *Huffpost.* [Consulta: 5 junio 2025]. Disponible en: https://www.huffingtonpost.es/global/un-pais-clave-otan-pone-jaque-rusia-revelar-planes-nucleares-secretos.html

Infantes Capdevila, G. (2023). Qué sabemos de los «hackers» rusos conocidos como Cold River [en línea]. *Newtral*. [Consulta: 5 junio 2025]. Disponible en: 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*. Recuperado el 12 de marzo de 2026, de https://www.iiss.org/publications/strategic-dossiers/russias-military-modernisation/

Kaspersky ICS CERT. **(2024)**. Threat Landscape for Industrial Automation Systems. Statistics for H2 2023 [en línea]. *Kaspersky*. [Consulta: 5 junio 2025]. Disponible en: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-Statistics-for-H2-2023-En.pdf

Knapczyk, P. y Kazymirskyi, N. (2024). The Russia-Ukraine Cyber War Part 2: Attacks Against Government Entities, Defense Sector, and Human Targets [en línea]. *Trustwave Spiderlabs / LevelBlue*. [Consulta: 5 junio 2025]. Disponible en: 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 [en línea]. *Kyiv Independent*. [Consulta: 6 junio 2025]. Disponible en: https://kyivindependent.com/osint-project-reports-another-failed-russian-nuclear-missile-test/

Marcelin, J. y Litnarovych, V. (2025). Rusia moderniza discretamente silos de misiles nucleares cerca de la frontera con Kazajistán, según documentos filtrados [en línea]. *United24Media* . [Consulta: 5 junio 2025]. Disponible en: 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 [en línea]. *Arms Control Association*. [Consulta: 6 junio 2025]. Disponible en: 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 [en línea]. *The War Zone*. [Consulta: 6 junio 2025]. Disponible en: 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 [en línea]. *Ciberprisma*. [Consulta: 2025]. Disponible en: https://ciberprisma.org/2025/01/07/riesgos-y-amenazas-ciberneticas-en-los-entornos-nucleares/

Panda Security. **(2024)**. Ciberamenazas nucleares: ¿realmente hay un riesgo real? Panda Security [en línea]. *Panda Security*. [Consulta: 5 junio 2025]. Disponible en: https://www.pandasecurity.com/es/mediacenter/ciberamenazas-nucleares-realmente-hay-riesgo-real/

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

—. (2014). Russian Strategic Nuclear Forces: Facilities and Deployment [en línea]. *Russian Strategic Nuclear Forces Project*. [Consulta: 5 junio 2025]. Disponible en: https://russianforces.org/book/

Ribeiro, A. (2025). NATO allies boost cyber defense coordination, focus on improving critical infrastructure resilience [en línea]. *Industrial Cyber.* [Consulta: 6 junio 2025] Disponible en: 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 [en línea]. *Atlantic Council.* [Consulta: 6 junio 2025]. Disponible en: 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, U.S. Army War College, 2004. Disponible en: https://press.armywarcollege.edu/monographs/32/

Swissinfo. (2023). El grupo de «hackers» norcoreano Andariel roba a Corea del Sur tecnologías de defensa [en línea]. *Swissinfo*. [Consulta: 5 junio 2025] Disponible en: 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? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States [en línea]. *International Security*. 41(4), pp. 50-92. [Consulta: 5 junio 2025]. Disponible en: https://doi.org/10.1162/ISEC_a_00274

Tucker, P. (2021). Russia's Avangard Hypersonic Missile Ready for Combat [en línea]. *Defense One*. [Consulta: 5 junio 2025]. Disponible en: www.defenseone.com

Ukrainian World Congress. (2024). Russia falters again in testing Sarmat nuclear missile [en línea]. *Ukrainian World Congress*. [Consulta: 6 junio 2025] Disponible en: https://www.ukrainianworldcongress.org/russia-falters-again-in-testing-sarmat-nuclear-missile/

Unal, B. y Lewis, P. (2018). *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences* [en línea]. Londres: Chatham House. [Consulta: 6 junio 2025]. Disponible en: https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf

Urdiroz, F. (2025). Entre algoritmos y alarmas: el impacto de la IA en la ciberseguridad [en línea].*Global Affairs*. Universidad de Navarra, [Consulta: 5 junio 2025]. Disponible en: https://www.unav.edu/web/global-affairs/entre-algoritmos-y-alarmas-el-impacto-de-la-ia-en-la-ciberseguridad

Artículo recibido: 6 de junio de 2025
Artículo aceptado: 15 de enero de 2026