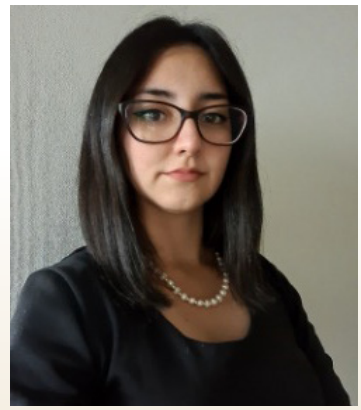
Escenarios Actuales, año 31, septiembre, N.º 1 (2026), pp. 99-119
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

El campo de batalla transparente: ciberamenazas, inteligencia artificial y disuasión en la seguridad de Estados Unidos y sus implicancias estratégicas para Chile



Denisse Olguín Arias[1]

Resumen

Cuando el código se convierte en un arma y los algoritmos en centinelas, la concepción tradicional de la seguridad nacional queda irremediablemente superada. La expansión del ciberespacio como quinto dominio de conflicto estratégico ha obligado a Estados Unidos a replantear desde sus fundamentos doctrinales la manera en que se protege su infraestructura crítica, proyecta poder y disuade a sus adversarios. El presente artículo examina, desde una perspectiva analítico-estratégica, tres vectores interconectados que impulsan esta arquitectura doctrinal de la ciberdefensa estadounidense entre 2022 y 2025, signada por la transición del multilateralismo cibernético hacia el soberanismo digital; la amenaza iraní como paradigma de actor asimétrico que combina persistencia técnica con objetivos geopolíticos escalables y la integración acelerada de inteligencia artificial en los sistemas de defensa cibernética con especial atención al caso Grok/GenAI.mil, sus oportunidades operativas y sus riesgos sistémicos no resueltos. Asimismo, se examinan las implicancias geopolíticas de estos desarrollos para el sistema internacional y, específicamente, para países de mediano desarrollo tecnológico como Chile, cuya reciente Ley Marco de Ciberseguridad (N.° 21.663,



Palabras clave
Ciberdefensa
Inteligencia Artificial
Disuasión Cibernética
Irán
Ciberseguridad

Keywords
Cyber Defense
Artificial Intelligence
Cyber Deterrence
Iran
Cybersecurity

1 Ingeniera en Automatización y Robótica de la Universidad Andrés Bello (UNAB), Máster en Ingeniería Aeronáutica de la Universidad Técnica Federico Santa María (UTFSM). Investigadora de Electrónica y TIC Centro de Estudios en Ciencia y Tecnología de la Academia Politécnica Militar (CECTAP) del Ejército de Chile y docente del mismo instituto.

2024) abre una ventana de oportunidad que las lecciones del caso estadounidense pueden contribuir a aprovechar con mayor eficacia. Se concluye que la ciberdefensa del siglo XXI exige la convergencia de capacidades técnicas de vanguardia, marcos normativos que las disciplinen, gobernanza robusta de la inteligencia artificial y alianzas que amplíen la superficie defensiva; un equilibrio que ni la potencia hegemónica ni sus socios menores han alcanzado todavía.

Abstract

When code becomes a weapon and algorithms serve as sentinels, the traditional conception of national security becomes irreversibly obsolete. The expansion of cyberspace as the fifth domain of strategic conflict has compelled the United States to reconsider, from its very doctrinal foundations, the way in which it protects its critical infrastructure, projects power, and deters its adversaries. This article examines, from an analytical-strategic perspective, three interconnected vectors that drive this reconfiguration: the doctrinal architecture of U.S. cyber defense between 2022 and 2025, marked by the transition from cyber multilateralism to digital sovereigntism; the Iranian threat as a paradigm of an asymmetric actor combining technical persistence with scalable geopolitical objectives; and the accelerated integration of artificial intelligence into cyber defense systems, with particular attention to the Grok/GenAI.mil case, its operational opportunities, and its unresolved systemic risks. Likewise, the article examines the geopolitical implications of these developments for the international system and, specifically, for medium technologically developed countries such as Chile, whose recent Cybersecurity Framework Law (No. 21.663, 2024) opens a window of opportunity that lessons drawn from the U.S. case may help leverage more effectively. The article concludes that twenty-first century cyber defense requires the convergence of cutting-edge technical capabilities, regulatory frameworks capable of disciplining them, robust artificial intelligence governance, and alliances that expand the defensive surface; a balance that neither the hegemonic power nor its smaller partners have yet achieved.

Introducción

Alrededor de la 1:30 p.m. del 5 de febrero de 2021, los operadores del sistema de control de la planta de tratamiento de agua de Oldsmar, Florida, observaron cómo el cursor de su pantalla se desplazaba sin intervención humana y alguien elevaba remotamente la concentración de hidróxido de sodio hasta niveles 100 veces superiores al umbral de seguridad.[2] El incidente fue contenido en minutos, pero ilustró con una elocuencia perturbadora lo que los documentos estratégicos tendían a expresar en términos abstractos: el ciberespacio no es un dominio virtual y separado de la realidad física, sino un campo de batalla transparente[3] a través del cual los adversarios pueden provocar daños materiales sin disparar un solo proyectil.

Dos años después, el 2 de marzo de 2023, la administración Biden-Harris publicó la *National*

2 PEISER, Jaclyn. A hacker tried to poison the water supply in Oldsmar, Florida, police said. The Washington Post. 9 de febrero de 2021, [En línea]. Disponible en: https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/

3 El concepto de campo de batalla transparente proviene de la teoría militar soviética de los años 80 sobre los "complejos de reconocimiento-ataque", también conocido como RUK (es la sigla del término ruso разведывательно-ударный комплекс (transliterado: razvedyvatel'no-udarny kompleks), que se traduce como "complejo de reconocimiento-ataque" o "complejo de reconocimiento-empeño", como lo tradujo Frías Sánchez), que sostenía que los avances en sensores permitirían detectar y localizar con precisión todo elemento presente en el campo de batalla (Vego, 1990). Para un análisis contemporáneo del concepto, véase Frías Sánchez (2021). En el dominio cibernético, este artículo adapta la idea para describir cómo las herramientas de monitoreo, atribución forense e inteligencia artificial incrementan la visibilidad sobre la actividad maliciosa, aunque persisten zonas de opacidad (como la atribución técnica y jurídica de un ataque) que actores como Irán explotan deliberadamente.

Cybersecurity Strategy,[4] el documento rector más ambicioso en materia de ciberseguridad elaborado hasta entonces por el gobierno federal estadounidense. Su premisa articulaba una doble verdad incómoda: que la ciberseguridad constituye un componente estructural de la seguridad nacional, y que el modelo vigente que cargaba sobre individuos, pequeñas empresas y operadores de infraestructura la responsabilidad de su propia protección, había distribuido el riesgo de forma injusta e insostenible. La estrategia proponía revertir esa ecuación, trasladando la carga hacia los actores más capaces: las grandes empresas tecnológicas y el propio Estado federal.

El panorama se complejizó de manera sustancial con la llegada de la administración Trump y la publicación de la *National Security Strategy* (NSS[5]) de 2025, que introdujo una reorientación doctrinal profunda.[6] El enfoque multilateral y normativo fue desplazado por un marco de realismo soberanista en el que la tecnología (incluida la inteligencia artificial) deja de ser un bien común global para convertirse en un instrumento de primacía nacional.

Simultáneamente, la escalada del conflicto Israel-Irán a lo largo de 2025 y 2026 ha convertido las amenazas cibernéticas iraníes en una presión cotidiana sobre la infraestructura crítica estadounidense, mientras la reducción del personal de la principal agencia defensiva del país, la CISA,[7] expone una brecha estructural entre la retórica de la superioridad y la realidad operativa de la defensa.

En el contexto señalado, este artículo analiza esa tensión en tres planos concéntricos: el macroestratégico (la transformación doctrinal entre Biden y Trump); el operativo (la amenaza iraní y la integración de inteligencia artificial en los sistemas de defensa) y el prospectivo (las implicancias geopolíticas para el sistema internacional y, de manera particular, para Chile).

El hilo conductor relacionado con la temática a presentar es una pregunta que la literatura especializada ha formulado con creciente urgencia: ¿puede la disuasión, concebida para un mundo de actores estatales racionales y armas convencionales, trasladarse con eficacia a un dominio donde la atribución es opaca, la escalada es involuntaria y los actores de capacidad media pueden producir efectos estratégicos de primera magnitud?

El ciberespacio como quinto dominio: asimetría, opacidad y ausencia normativa

La incorporación del ciberespacio como quinto dominio de operaciones militares no fue el producto de una visión anticipatoria de los

4 COKER, Harry Jr. Annual Report on the United States Cybersecurity Posture. Washington D.C.: Office of the National Cyber Director. 2024. [En línea]. Disponible en: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf. El informe afirma que EE.UU. se halla "en medio de una transformación fundamental" de sus defensas cibernéticas.

5 NATIONAL SECURITY STRATEGY (NSS): documento estratégico elaborado por un gobierno para definir los objetivos, prioridades y acciones relacionadas con la protección de la seguridad nacional, incluyendo aspectos políticos, militares, económicos, tecnológicos y de ciberseguridad.

6 En la doctrina militar estadounidense, el ciberespacio fue formalmente reconocido como quinto dominio de operaciones militares, junto con la tierra, el mar, el aire y el espacio, mediante la Estrategia Cibernética del DoD de 2011, posteriormente consolidada en las revisiones de 2015, 2018 y 2023.

7 CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), en español, Agencia de Ciberseguridad y Seguridad de Infraestructura: organismo del gobierno de los Estados Unidos encargado de proteger las infraestructuras críticas, los sistemas digitales y las redes gubernamentales frente a amenazas cibernéticas y riesgos de seguridad.

estados mayores, sino el reconocimiento tardío de una realidad que los conflictos del siglo XXI habían impuesto por la fuerza de los hechos[8].

Desde los ataques de denegación de servicio contra Estonia en 2007, primer caso documentado de ciberagresión con motivación geopolítica, hasta el ataque NotPetya de 2017, que con un solo módulo de malware encadenado a una actualización fiscal ucraniana causó daños estimados en 10.000 millones de dólares a nivel global,[9] el ciberespacio ha demostrado ser un multiplicador de fuerza sin precedentes: capaz de producir efectos estratégicos comparables a los de una campaña militar convencional, pero a una fracción de su coste y con un grado de plausible negación que ningún sistema de armas físico puede ofrecer.

La arquitectura del conflicto en este dominio descansa sobre tres características estructurales que lo distinguen radicalmente de los dominios tradicionales.

La primera es la asimetría de costos: un actor que invierta decenas de miles de dólares en el desarrollo o adquisición de un exploit[10] sofisticado puede paralizar infraestructuras industriales o redes gubernamentales cuya construcción y operación representan miles de millones. Esta asimetría rompe la lógica clásica de la disuasión, que presupone que el atacante y el defensor compiten en costos relativamente comparables.

La segunda es la opacidad atributiva: identificar con certeza jurídica y política al autor de un ciberataque requiere capacidades de inteligencia técnica de alto nivel, semanas o meses de investigación y la voluntad política de asumir las consecuencias diplomáticas de una atribución pública.[11] Esta opacidad crea un espacio estratégico de impunidad deliberada que los actores estatales, y en particular aquellos que operan en la zona gris entre la guerra y la paz, explotan de forma sistemática.

La tercera es la ausencia de un régimen normativo estabilizador: a diferencia del dominio nuclear, donde décadas de negociaciones produjeron tratados que codificaron límites aceptables de comportamiento entre las grandes potencias, el ciberespacio carece de un andamiaje normativo equivalente. Los esfuerzos de la comunidad internacional, desde el Grupo de Expertos Gubernamentales de la ONU hasta las negociaciones en la Conferencia de Desarme, han producido declaraciones de principios sin mecanismos vinculantes de verificación ni consecuencias definidas para la infracción, lo que deja abierta una brecha normativa que los actores más dispuestos a explotar la ambigüedad aprovechan de forma sistemática.

8 KLIMBURG, Alexander. The Darkening Web: The War for Cyberspace. New York: Penguin Press, 2017, p. 58.

9 Greenberg, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED, 22 de agosto de 2018, [En línea]. Disponible en: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ La estimación de daños por más de USD 10.000 millones corresponde a una evaluación de la Casa Blanca, confirmada por Tom Bossert, ex asesor de seguridad nacional del presidente Trump.

10 Exploit: herramienta, código o técnica utilizada para aprovechar una vulnerabilidad en un sistema informático con el fin de obtener acceso no autorizado, alterar su funcionamiento o ejecutar un ataque. Por ejemplo, un exploit puede aprovechar una falla en un servidor para ingresar remotamente a una red industrial o gubernamental.

11 RID, Thomas. Cyber War Will Not Take Place. Oxford University Press. 2023. [En línea]. Disponible en: https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf. El autor desarrolla el argumento de que los ciberataques raramente alcanzan el umbral del "acto de guerra" en sentido clausewitziano, lo que complejiza la lógica disuasoria.

La convergencia de estas tres características genera lo que el teórico Lucas Kello ha denominado una condición de unpeace: un estado de conflicto persistente y difuso que no alcanza el umbral formal de la guerra declarada, pero que erosiona continuamente la seguridad, la confianza y la estabilidad de los actores implicados.[12] En esas condiciones, la arquitectura de ciberdefensa de una potencia como Estados Unidos no puede reducirse a la acumulación de capacidades técnicas: debe integrar doctrina estratégica, marcos jurídicos que autoricen respuestas proporcionales, mecanismos de coordinación con el sector privado (que controla la gran mayoría de la infraestructura crítica nacional) y una teoría coherente de la disuasión aplicada a un dominio que resiste sistemáticamente la lógica de los modelos clásicos. El fracaso en cualquiera de esos planos no es una deficiencia técnica; es una vulnerabilidad estratégica.

De la cooperación a la soberanía: la arquitectura doctrinal de la ciberdefensa estadounidense

El período 2022-2025 ha sido uno de los más fértiles en producción doctrinal de ciberseguridad en la historia de Estados Unidos, aunque también ha presentado desafíos en términos de coherencia estratégica. La *National Cybersecurity Strategy* de marzo de 2023 estableció un marco ambicioso de cinco pilares: defensa de infraestructura crítica, desarticulación de actores de amenaza, creación de incentivos de mercado para la resiliencia, inversión en tecnología de largo plazo y cooperación internacional; y articuló por primera vez el principio de responsabilidad diferenciada: quienes poseen mayor capacidad técnica y mayor influencia sobre el ecosistema digital deben asumir una carga proporcional de la defensa colectiva.[13]

Ese mismo año (2023), el Departamento de Defensa publicó el resumen de su propia estrategia cibernética[14] –que ratificó la política de Defend Forward,[15] comprometer a los adversarios en sus propias redes antes de que puedan ejecutar ataques– y amplió el mandato del Comando Cibernético (CYBERCOM[16]) para conducir operaciones de caza persistente en redes de terceros países con su consentimiento.

La llegada de la administración Trump y la publicación de la NSS-2025 introdujeron una reorientación que va más allá del cambio de énfasis político: constituye una ruptura epistemológica en la manera en que el Estado estadounidense concibe el ciberespacio. Donde la estrategia de 2023 concebía el ecosistema digital como un bien colectivo que el Estado debe contribuir a gobernar, la NSS-2025 lo reencuadra como un

12 KELLO, Lucas. The Virtual Weapon and International Order. New Haven: Yale University Press. 22 de agosto de 2017, [En línea]. Disponible en: https://www.academia.edu/61597942/The_Virtual_Weapon_and_International_Order. El autor acuñó el concepto de unpeace para describir un estado de conflicto persistente y difuso situado por debajo del umbral formal de la guerra declarada.

13 El término Defend Forward designa la doctrina de U.S. Cyber Command que consiste en comprometer actividad a los adversarios en sus propias redes antes de que puedan lanzar ataques contra infraestructura estadounidense. Fue normalizado en la Estrategia Cibernética del DoD de 2018 y ratificado en la de 2023.

14 MARQUÉZ DE LA RUBIA, Francisco. La Estrategia de Seguridad Nacional de los Estados Unidos. 2025: análisis y comparativa con la ESN 2022. IEEE-CESEDEN. 10 de diciembre de 2025, [En línea]. Disponible en: https://www.defensa.gob.es/ceseden/-/ieee/

15 ABC NEWS. DHS shutdown fuels cybersecurity concerns as Iran-linked cyberattacks continue across US. 3 de abril de 2026, [En línea]. Disponible en: https://abcnews.com/Politics/dhs-sutdown-fuel-cybersecurity-concerns-iran-linked-cyberattacks/story?id=131546421

16 CYBERCOM (United States Cyber Command): comando militar encargado de dirigir y coordinar operaciones de ciberdefensa y ciberseguridad para proteger las redes, sistemas e infraestructuras digitales del Departamento de Defensa de los Estados Unidos.

dominio de ventaja competitiva que el Estado debe controlar.[17]

En este contexto, el análisis del Instituto Español de Estudios Estratégicos – CESEDEN (Centro Superior de Estudios de la Defensa Nacional) sostiene que esta visión adopta un nacional-industrialismo estratégico que prioriza la autonomía tecnológica, el control de las cadenas de suministro y la supremacía en inteligencia artificial bajo una lógica de primacía soberana. Como consecuencia, la cooperación multilateral en ciberdefensa pierde relevancia frente a la competencia tecnológica entre bloques, mientras que los estándares compartidos de ciberseguridad y la participación en foros

internacionales pasan a evaluarse desde una perspectiva principalmente instrumental.

Esta tensión doctrinal tiene manifestaciones concretas e inmediatas. La más preocupante es la reducción severa del personal de la CISA (organismo responsable de coordinar la ciberdefensa del territorio nacional), con una fracción significativa de su plantilla fuera de funciones a principios de 2026, precisamente en el momento de mayor presión operativa por las amenazas iraníes. El Dr. Frederic Lemieux, profesor de gestión de riesgo cibernético en la Universidad de Georgetown, calificó esta decisión como *"absolutamente peligrosa"*, advirtiendo que reducir la capacidad defensiva cuando un adversario conocido intensifica sus operaciones invierte la lógica elemental de la gestión de riesgos.[18] La paradoja que esto encierra es reveladora: la NSS-2025 proclama la supremacía tecnológica como pilar de la seguridad nacional, al tiempo que desfinancia la agencia cuya misión esencial es traducir esa aspiración en protección efectiva.

La tabla N.°1 sistematiza las diferencias operativas entre el enfoque defensivo y el enfoque ofensivo-disuasivo de la ciberdefensa estadounidense:

Dimensión	Enfoque defensivo	Enfoque ofensivo / disuasivo
Objetivo	Proteger redes propias.	Degradar capacidades adversarias antes del ataque.
Mecanismo central	Parchado, monitoreo, arquitectura ZTNA.[19]	Defend Forward, hunt forward operations.
Actor principal	CISA, sector privado, FCEB.[20]	CYBERCOM, NSA, DoD[21] CDAO.[22]

17 FBI, CISA DC3. Joint Cybersecurity Advisory AA24-241A: Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations. Agosto 2024, [En línea]. Disponible en: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

18 Cybersecurity & Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA). Updated Advisory AA23-335A: IRGC-Affiliated Cyber Actors Exploits PLCs in Multiple Sectors, including US wáter and wastewater systems facilities. 18 de dicimenre de 2024, [En Línea]. Disponible en: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

19 ZTNA (Zero Trust Network Access): modelo de seguridad informática que restringe el acceso a aplicaciones y recursos digitales mediante la verificación continua de usuarios y dispositivos, asumiendo que ninguna conexión debe considerarse confiable por defecto, incluso dentro de una red interna.

20 FCEB (Federal Civilian Executive Branch): conjunto de agencias y organismos civiles pertenecientes al poder ejecutivo del gobierno federal de los Estados Unidos, responsables de administrar y ejecutar políticas públicas en distintas áreas no militares.

21 DoD (Department of Defense): organismo gubernamental encargado de coordinar y supervisar las fuerzas armadas y las operaciones de defensa nacional de un país, especialmente en referencia al Departamento de Defensa de los Estados Unidos.

22 CDAO (Chief Digital and Artificial Intelligence Office): organismo encargado de coordinar e impulsar estrategias relacionadas con tecnologías digitales, análisis de datos e inteligencia artificial, especialmente en ámbitos de defensa, innovación y modernización tecnológica.

Dimensión	Enfoque defensivo	Enfoque ofensivo / disuasivo
Marco legal habilitante	CIRCA 2022, FCEB directives, CPGs	Orden Ejecutiva, NDAA,[23] EO 14028.
Rol de la IA	Detección de anomalías, XDR,[24] triaje	Automatización de respuesta, OSINT[25] sintético.
Limitación estructural	Depende de parches adoptados por privados	Riesgo de escalada no intencional.

Tabla N.°1: Dimensiones comparativas de la ciberdefensa estadounidense.

Fuente: Elaboración propia.

La amenaza iraní: coerción asimétrica, infraestructura crítica y la era de la IA ofensiva

Si hubiera que identificar un caso que reúna las características más desafiantes del ciberconflicto moderno (como la asimetría de recursos, la motivación geopolítica escalable, la disposición al daño físico y la capacidad de adaptación táctica continua), ese caso sería Irán. A pesar de destinar a sus capacidades cibernéticas ofensivas una inversión considerablemente menor que la empleada por Estados Unidos en ciberdefensa, el ecosistema cibernético iraní, articulado en torno al Islamic Revolutionary Guard Corps (IRGC) y grupos *hacktivistas* afines, ha demostrado capacidad para afectar a potencias industriales avanzadas, difuminando la frontera entre el conflicto cibernético y la acción cinética.

Los antecedentes son ilustrativos de esa trayectoria. La campaña *Shamoon* de 2012, que inutilizó aproximadamente 30.000 computadoras de Saudi Aramco,[26] fue en su momento el ciberataque más destructivo jamás ejecutado contra una empresa privada. Entre 2012 y 2013, el grupo vinculado al IRGC conocido como Izz ad-Din al-Qassam Cyber Fighters ejecutó una serie de ataques de denegación de servicio distribuido (DDoS) contra al menos 46 instituciones financieras estadounidenses (incluyendo Bank of America, JPMorgan Chase y Wells Fargo), causando interrupciones sostenidas que obligaron a las entidades afectadas a destinar cuantiosos recursos en medidas de mitigación y respuesta defensiva.[27] En 2021, el mismo ecosistema comprometió el sistema de abastecimiento de agua de Oldsmar, Florida, elevando remotamente la concentración de hidróxido de sodio a niveles que, de no haber sido detectados, habrían podido causar daños graves a la salud pública.

La fase más reciente de la actividad cibernética atribuida a actores iraníes evidencia un mayor

23 NDAA (National Defense Authorization Act): legislación aprobada anualmente en los Estados Unidos que establece el presupuesto, las políticas y las prioridades relacionadas con las fuerzas armadas y la seguridad nacional.

24 XDR (Extended Detection and Response): solución de ciberseguridad que integra y correlaciona información proveniente de múltiples sistemas y dispositivos para detectar, analizar y responder de manera centralizada a amenazas y ataques informáticos.

25 OSINT (Open Source Intelligence): proceso de recopilación, análisis y utilización de información obtenida de fuentes públicas y accesibles, como sitios web, redes sociales, publicaciones, bases de datos y medios digitales, con fines de investigación, seguridad o análisis estratégico.

26 PERLROTH, Nicole. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, The New York Times. 23 de octubre de 2012, [En línea]. Disponible en: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html La cifra de aproximadamente 30.000 computadoras inutilizadas fue confirmada oficialmente por Saudi Aramco en comunicado del 27 de agosto de 2012.

27 U.S. Department of Justice, United States v. Ahmad Fathi et al., Indictment, S.D.N.Y., 24 de marzo de 2016, pp. 4–7, [En línea]. Disponible en: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

nivel de desarrollo operativo. De acuerdo con un aviso conjunto emitido por el FBI, la CISA y el DC3[28] en agosto de 2024, estos actores continuaban dirigiendo actividades hacia organizaciones estadounidenses de sectores considerados críticos, entre ellos educación, finanzas, salud, defensa y gobiernos locales. Para ello, empleaban técnicas de exploración de redes mediante herramientas como Shodan y aprovechaban vulnerabilidades CVE[29] previamente identificadas en dispositivos de fabricantes como Check Point Software Technologies, Palo Alto Networks y Citrix.[30]

La sofisticación no reside tanto en el uso de exploits de día cero como en la sistematicidad y la disciplina operativa: el actor iraní es paciente, metódico y capaz de sostener intrusiones silenciosas durante períodos prolongados antes de activar su carga útil.

El episodio de mayor impacto estratégico del período reciente fue la campaña *CyberAv3ngers* (grupo afiliado al IRGC[31]) ejecutada entre noviembre de 2023 y enero de 2024, en el contexto del conflicto Israel-Gaza. Los atacantes comprometieron controladores lógicos programables[32] (PLC)[33] de fabricación israelí ubicados en instalaciones de agua y aguas residuales, manufactura de alimentos y bebidas y servicios de salud en territorio estadounidense. Los dispositivos explotados tenían en común una característica elemental: habían sido desplegados con contraseñas de fábrica o sin ninguna protección en puertos TCP[34] predeterminados accesibles desde internet.[35] Este detalle es analíticamente fundamental: una potencia de segundo orden fue capaz de afectar infraestructura crítica de la primera potencia mundial no porque sus capacidades técnicas sean superiores, sino también porque las prácticas de higiene cibernética implementadas por los operadores de dicha infraestructura aún presentan oportunidades de fortalecimiento y mejora.

La CISA y sus agencias socias advirtieron en junio de 2025 que estos actores continuaban explorando vulnerabilidades en redes de tecnología

28 DC3: Centro de Delitos Cibernéticos del Departamento de Defensa de los Estados Unidos (Department of Defense Cyber Crime Center).

29 CVE: Common Vulnerabilities and Exposures (Vulnerabilidades y Exposiciones Comunes). Sistema de identificación estandarizada de vulnerabilidades de seguridad mantenido por MITRE Corporation y financiado por la CISA.

30 CISA. Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest. 30 de junio de 2025, [En línea]. Disponible en: https://www.ic3.gov/CSA/2025/250630.pdf

31 IRGC: Islamic Revolutionary Guard Corps: organización militar y de seguridad de Irán creada para proteger el sistema político y los intereses estratégicos del país, participando en operaciones militares, inteligencia y ciberdefensa.

32 Un PLC (Programmable Logic Controller o Controlador Lógico Programable) es un dispositivo electrónico industrial diseñado para automatizar y controlar procesos en máquinas y sistemas industriales. Su función principal es recibir señales de entrada desde sensores o dispositivos, procesarlas según un programa previamente configurado y generar señales de salida para accionar motores, válvulas, luces u otros actuadores. Estos dispositivos son ampliamente utilizados en automatización industrial debido a su confiabilidad, rapidez y capacidad de operar en entornos exigentes.

33 CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS). Iran Conflict Heightens Cyber Threats to U.S. Energy Infrastructure. 9 de abril de 2026, [en línea]. Disponible en: https://www.csis.org/analysis/iran-conflict-heightens-cyber-threats-us-energy-infrastructure. El informe cita datos de Check Point Research sobre el incremento de ataques al sector energético.

34 El puerto TCP (Transmission Control Protocol) es un identificador numérico utilizado para diferenciar servicios y aplicaciones dentro de un dispositivo conectado a una red. Cada puerto permite que un servicio específico reciba y procese datos provenientes del tráfico de red, facilitando la comunicación entre equipos. Forma parte del modelo de comunicación TCP/IP, el cual constituye la base del funcionamiento actual de Internet.

35 FOUNDATION FOR DEFENSE OF DEMACRACIES (FDD). How an Iranian Cyberattack Hit US Local Goverments. 14 de abril de 2026, [En línea]. Disponible en: https://www.fdd.org/analysis/2026/04/14/how-an-iranian-cyberattack-hit-us-local-goverments/

operacional (OT[36]) con énfasis en dispositivos con credenciales débiles o predeterminadas.[37] El CSIS reportó que el sector energético estadounidense enfrentó en 2024 un promedio de más de 1.160 intentos de ataque semanales por organización, un incremento del 70% respecto al año anterior, con actores iraníes, chinos y rusos, representando en conjunto aproximadamente dos tercios de los ataques atribuidos al sector entre 2010 y 2024.[38]

Lo que distingue al actor iraní de China o Rusia en el ciberespacio no es solo su capacidad técnica, inferior en ambos casos, sino su disposición al uso inmediato del ciberespacio como instrumento de coerción geopolítica en tiempo real. Mientras China opera con una lógica de preposicionamiento latente y Rusia combina el ciberataque con operaciones de influencia en conflictos declarados, como se examinará más adelante, Irán activa sus capacidades cibernéticas como herramienta de presión directa en momentos de crisis, generando efectos disuasorios propios frente a actores más poderosos. La consecuencia es un adversario de naturaleza híbrida: ni tan capaz como China ni tan integrado en una doctrina de guerra convencional como Rusia, pero potencialmente más peligroso a corto plazo por su disposición a cruzar umbrales que otros actores preferirían evitar.

La perspectiva de una IA iraní ofensiva amplifica esas preocupaciones. Según la Foundation for Defense of Democracies, la inteligencia artificial definirá la próxima fase de los ciberataques iraníes, haciéndolos más rápidos, más baratos y considerablemente más difíciles de atribuir.[39] Irán ha demostrado ya el uso extensivo de IA para campañas de desinformación; incluyendo la generación de contenido dirigido a poblaciones israelíes y es razonablemente previsible que esas capacidades migren hacia el ámbito del ciberataque adaptativo, donde los modelos de aprendizaje profundo pueden generar variantes de malware que evaden los sistemas de detección entrenados con firmas históricas.[40]

Inteligencia artificial en la ciberdefensa: GenAI.mil, el caso Grok y la gobernanza pendiente

En julio de 2025, el Departamento de Defensa ejecutó la decisión estratégica más significativa en materia de IA aplicada a la defensa desde la

36 Operational Technology / Tecnología Operacional (OT): conjunto de sistemas, dispositivos y software utilizados para supervisar, controlar y automatizar procesos físicos e industriales en entornos como fábricas, plantas eléctricas, sistemas de transporte e infraestructuras críticas. La OT integra tecnologías como sensores, PLC, SCADA y sistemas de control industrial para operar maquinaria y procesos en tiempo real.

37 Industrial Cyber. CSIS flags Iran's shift from episodic cyberattacks to sustained campaign against critical infrastructure. 9 de abril de 2026, [En línea]. Disponible en: https://industrialcyber.co/industrial-cyber-attacks/csis-flags-irans-shift-from-episodic-cyberattacks-to-sustained-against-critical-infrastructure/

38 DOD CDAO. CDAO Announces Parnetships with Frontier AI Companies to Address Critical National Security Challenges. Defense News. Julio 2025, [En línea]. Disponible en: https://www.defensenews.com/pentagon/2025/07/15/pentagon-taps-four-commercial-tech-firms-to-expand-military-use-of-ai/

39 U.S. Department of War. The War Department to Expand AI Arsenal on GenAi.mil with xAI. 22 de diciembre de 2025, [En línea]. Disponible en: https://www.war.gov/News/Releases/Release/Article/4366573/

40 IL5 (Impact Level 5) es una clasificación de seguridad en la nube del DoD que habita el manejo de información no clasificada controlada (CUI) y datos de sistemas de seguridad nacional. Su equivalente en terminología de la comunidad de inteligencia es la categoría SBU (Sensitive But Unclassified).

creación del Proyecto Maven en 2017: suscribir contratos simultáneos por hasta 200 millones de dólares cada uno con *Google, xAI, Anthropic y OpenAI,* para el desarrollo de flujos de trabajo de IA agentiva[41] en misiones de seguridad nacional.[42] Esta decisión no representa meramente la adopción de una nueva herramienta; señala un cambio estructural en la manera en que el Departamento de Defensa concibe la ventaja informativa: no como el producto del análisis humano apoyado por máquinas, sino como el resultado de sistemas que piensan, deciden y actúan a velocidades y escalas que superan las capacidades cognitivas humanas.

En diciembre del mismo año, el Departamento de Guerra (nueva denominación bajo la administración Trump) anunció la incorporación de la suite xAI para Gobierno a GenAI.mil, la plataforma de IA institucional del Pentágono. Bajo este acuerdo, los modelos de la familia Grok quedan integrados en los flujos de trabajo cotidianos de los tres millones de funcionarios militares y civiles del departamento,[43] con certificación al Nivel de Impacto 5 (IL5),[44] que habilita el manejo de Información No Clasificada Controlada (CUI[45]) en entornos de alta sensibilidad. El Departamento justificó la integración en el concepto de *information advantage*: la capacidad de procesar y actuar sobre información de manera más rápida y precisa que el adversario. La presencia de Grok incluye acceso en tiempo real a la plataforma X, lo que el Departamento calificó de *"ventaja informativa decisiva"* para el personal operativo.[46]

Este movimiento ha desencadenado un debate institucional de primera relevancia. La senadora Elizabeth Warren dirigió en septiembre de 2025 una carta al Secretario de Defensa Hegseth, identificando cuatro vectores de riesgo: la posibilidad de que Elon Musk, en su calidad de exasesor especial del ejecutivo, hubiera obtenido acceso a datos del DoD utilizables para entrenar los modelos de xAI, generando una ventaja competitiva indebida sobre los demás contratistas,[47] es decir, el riesgo de concentración monopolística en un sector estratégico; los reportes documentados de que Grok genera resultados erróneos y desinformación

41 La IA agentiva es un tipo de inteligencia artificial diseñada para actuar de manera autónoma con el fin de cumplir objetivos específicos, tomando decisiones, planificando acciones y adaptándose según el contexto. A diferencia de los sistemas tradicionales que solo responden a instrucciones puntuales, una IA agentiva puede ejecutar tareas complejas de forma continua, interactuar con herramientas externas y coordinar múltiples pasos para alcanzar una meta determinada. Este enfoque es utilizado en asistentes inteligentes avanzados, automatización de procesos y sistemas autónomos basados en inteligencia artificial.

42 xAI. xAI for Government: US Department of War Partnership. Diciembre de 2025, [En línea]. Disponible en: https://x.ai./news/us-gov-dept-of-war

43 Warren, Elizabeth. Letter to Secretary Hegseth Regarding Integration of Grok into DOD Operations. U.S. Senate. 10 de septiembre de 2025, [En línea]. Disponible en: https://www.warren.senate.gov/imo/media/doc/letter_to_pentagon_regarding_integration_of_grok_91025.pdf

44 DefenseScoop. Sen. Warren letter to Hegseth on Musk-xAI DoD Contract. 11 de septiembre de 2025, [En línea]. Disponible en: https://defensescoop.com/2025/09/11/sen-warren-letter-hegseth-musk-xai-dod-contract/

45 Controlled Unclassified Information (CUI): categoría de información sensible que, aunque no posee clasificación confidencial o secreta, requiere controles especiales de manejo, almacenamiento y distribución para proteger su acceso y uso no autorizado.

46 SatNews. The Pentagon's Faustian Bargain: Buying Speed, Building a Monopoly. 24 de diciembre de 2025, [En línea]. Disponible en: https://satnews.com/2025/12/24/the-pentagons-faustian-bargain-buying-speed-building-a-monopoly/

47 U.S. Cyber Command. Persistent Engagement and Defending Forward. Fort Meade, MD: CYBERCOM. 2023. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/. El documento articula la doctrina de la "competencia persistente" como alternativa a la disuasión clásica en el ciberespacio.

y la generación de contenido antisemita y ofensivo en incidentes previos al contrato.[48] La respuesta del Pentágono fue telegráfica: el contrato con xAI es parte de un ecosistema plural que incluye también a *Google, Anthropic y OpenAI,* y su propósito es acelerar la ventaja tecnológica de las fuerzas armadas.

El análisis estratégico más severo, sin embargo, apunta a un riesgo más profundo que la idoneidad de un modelo específico: la emergencia de lo que algunos analistas han denominado el Musk Stack, una arquitectura en la que una sola entidad privada controla simultáneamente el lanzamiento orbital *(SpaceX-Falcon 9)*, la infraestructura de comunicaciones satelitales *(Starlink-Starshield)*, el análisis de inteligencia de fuentes abiertas *(xAI-Grok)* y la conectividad táctica de la cadena de mando.[49]

Históricamente, ningún actor privado había detentado simultáneamente el control sobre todos los eslabones de la cadena logística y de información de las fuerzas armadas de una potencia hegemónica. En caso de una disputa contractual, los mecanismos de dependencia creados harían que ese desacuerdo dejara de ser una negociación comercial para convertirse en una crisis de mando y control de consecuencias imprevisibles.

Es importante, no obstante, evitar que la controversia sobre Grok oscurezca el valor estratégico genuino de la IA en ciberdefensa. Las aplicaciones de mayor impacto operativo están bien establecidas en la literatura especializada: la detección de anomalías de comportamiento en redes mediante arquitecturas de *extended detection and response* (XDR), que pueden identificar indicadores de compromiso antes de que el atacante active su carga útil: el análisis de tráfico de red basado en aprendizaje profundo para la detección de intrusiones en tiempo real, la correlación automatizada de eventos de seguridad procedentes de miles de sensores dispersos en una arquitectura de infraestructura crítica y la generación sintética de escenarios de amenaza para el entrenamiento de analistas y la validación de protocolos de respuesta.

En todos los casos señalados, la IA ofrece ventajas de escala y velocidad que ningún equipo humano, por numeroso y cualificado que sea, puede replicar. El desafío no es si adoptar IA en ciberdefensa, sino cómo estructurar la supervisión humana en los puntos de decisión críticos para evitar que la velocidad algorítmica se convierta en un acelerador involuntario de la escalada.

Las paradojas de la disuasión cibernética

La disuasión nuclear, en su formulación canónica, opera sobre una premisa simple: si el adversario cree que un ataque desencadenará una respuesta que destruirá lo que más valora, se abstendrá de atacar. Esta lógica, aunque imperfecta y cargada de supuestos discutibles sobre la racionalidad de los actores, funcionó durante décadas como estabilizador del orden internacional. Su transposición al ciberespacio, sin embargo, choca contra resistencias

48 CSO Online. How the US DOD Cyber Strategy changes national cyber defense. 2024, [En línea]. Disponible en: https://www.csoonline.com/article/655937/how-the-us-dod-cyber-strategy-changes-national-cyber-defense.html

49 La disuasión por negación (deterrence by denial) busca convencer al adversario de que el ataque no podrá alcanzar sus objetivos porque las defensas lo impedirán. La disuasión por represalia (deterrence by punishment) opera mediante la amenaza de imponer costos inaceptables al atacante. En el ciberespacio ambas modalidades encuentran obstáculos estructurales distintos.

estructurales que la hacen, cuando menos, radicalmente más compleja y, en muchos casos, directamente inaplicable en su forma original.[50]

La primera paradoja de la disuasión cibernética es la del señalamiento sin revelación: para disuadir, es necesario que el adversario crea que se tiene capacidad de respuesta, pero revelar esa capacidad (en naturaleza, alcance y objetivos potenciales) reduce o elimina la ventaja ofensiva que la hace creíble. Un arsenal nuclear puede mostrarse en un desfile militar sin que eso deteriore su efectividad disuasoria; una operación de *Defend Forward* que se hace pública pierde buena parte de su valor operativo. La respuesta doctrinal del CYBERCOM ha sido construir una disuasión por reputación: acumular un historial de respuestas suficientemente costosas para el adversario sin especificar sus modalidades, apostando a que el adversario racional inferirá capacidades que prefiere no probar.[51]

La segunda paradoja es la de la invisibilidad del éxito defensivo: cuando la CISA bloquea 2.620 millones de intentos de ataque en un año,[52] ese éxito no se traduce en disuasión porque el atacante puede interpretar cada bloqueo como un fracaso técnico propio en lugar de una señal de la fortaleza defensiva del adversario. La disuasión por negación, es decir, convencer al adversario de que sus ataques no alcanzarán sus objetivos porque las defensas lo impedirán,[53] requiere que el fracaso sea percibido como consecuencia de las capacidades del defensor. Sin algún grado de comunicación estratégica deliberada, la defensa exitosa es silenciosa, en consecuencia, será disuasoriamente estéril.[54]

La tercera y más urgente paradoja es la de la automatización sin control: los sistemas de IA que hacen posible detectar y responder a ciberataques en milisegundos son los mismos que pueden desencadenar acciones ofensivas sobre la base de falsas atribuciones, falsos positivos algorítmicos o interpretaciones erróneas de la intención adversarial. En el dominio convencional, el error humano en la cadena de autorización tiene límites físicos que reducen la velocidad de la escalada. En el dominio cibernético potenciado por IA, esos límites desaparecen. Un sistema que detecta una intrusión y responde automáticamente con una contramedida ofensiva puede haber iniciado un ciclo de escalada mutua antes de que ningún decisor humano haya tenido la oportunidad de evaluar la situación. La NSS-2025, con su énfasis en la superioridad

50 Marquéz de la Rubia, Francisco. *Op. cit.*, pp. 8-11.

51 Ministerio del Interior y Seguridad Pública de Chile. Ley N.° 21.663 Marco sobre Ciberseguridad e Infraestructura Crítica de la información. Santiago: Diario Oficial de la República de Chile. La ley fue promulgada el 8 de marzo de 2024 y establece la Agencia Nacional de Ciberseguridad (ANCI).

52 CSIRT NACIONAL DE Chile. Informe de tendencias en ciberseguridad 2024. Santiago: Ministerio del Interior y Seguridad Pública. 2024, [En línea]. Disponible en: http://www.csirt.gob.cl

53 Organización de los Estados Unidos Americanos (OEA) / Banco Interamericano de Desarrollo (BID). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington D.C.: OEA/BID. 2020. [En línea]. Disponible en: https://doi.org/10.18235/0002513

54 NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE. 2023 NSA Cybersecurity Year in Review. Fort Meade, MD: NSA. [En línea]. Disponible en: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3621654/nsa-publishes-2023-cybersecurity-year-in-review/

tecnológica y la acción rápida, no ofrece respuestas a esta paradoja, de hecho, su lógica de acumulación de capacidades tiende a exacerbarla.

La arquitectura de ciberdefensa más eficaz, en consecuencia, no es la más ofensiva ni la más automatizada, sino la que resuelve con mayor inteligencia el equilibrio entre velocidad de respuesta y supervisión humana significativa, entre capacidad disuasoria y transparencia estratégica calibrada, y entre autonomía tecnológica y cooperación con aliados que amplían la superficie de detección. Ninguna de estas tensiones admite soluciones técnicas puras; todas son, en última instancia, decisiones de diseño institucional y político.

Implicancias geopolíticas: la ciberseguridad en la era de la rivalidad entre potencias.

La NSS-2025 reordena el tablero estratégico global en torno a tres vectores: la competencia con China como eje estructurante de la política exterior, el equilibrio pragmático con Rusia orientado a la gestión rápida del conflicto ucraniano, y la contención de actores revisionistas regionales como Irán, con el hemisferio occidental y el Indo-Pacífico como teatros preferentes.[55] En ese marco, la ciberseguridad no es un dominio sectorial más, es la infraestructura invisible que atraviesa todos los demás, el sistema circulatorio de la competencia económica, industrial y militar del siglo XXI. Las cadenas de suministro tecnológicas, los semiconductores, los modelos de IA y las plataformas de datos no son solo activos económicos, son simultáneamente vectores de vulnerabilidad estratégica cuya exposición puede determinar el resultado de conflictos que nunca lleguen a producir un disparo.

En el caso de China, la preocupación central de la inteligencia estadounidense no es la disrupción inmediata, sino el pre-posicionamiento estratégico de largo plazo: la infiltración silenciosa en redes críticas de energía, telecomunicaciones y transporte para ser activadas en caso de conflicto abierto. La campaña *Volt Typhoon*, que según el CSIS ha dominado los análisis de inteligencia sobre la República Popular China en los últimos años[56], ilustra con nitidez esa lógica: no producir daño inmediato, sino acumular acceso latente que confiera opciones en un escenario de escalada futura. Frente a ese adversario, la respuesta más eficaz no es la disuasión activa sino la resiliencia sistémica y la reducción de la superficie de ataque.

En el caso de Rusia, la reorientación de la NSS-2025 tiene consecuencias directas para el equilibrio cibernético global: al subordinar el apoyo a Ucrania a la gestión rápida del conflicto, con el objetivo de liberar recursos para el Indo-Pacífico,[57] Estados Unidos señala que la ciberresiliencia ucraniana, construida con una inversión significativa de cooperación técnica occidental, podría quedar comprometida por un acuerdo de cesación de hostilidades que no garantice sus condiciones de seguridad digital. Esto no es un detalle periférico: la capacidad de Ucrania para resistir operaciones cibernéticas rusas durante el conflicto armado

55 Marquéz de la Rubia, Francisco, *op. cit.*
56 National Security Agency / Central Security Service. 2023, *op. cit*
57 Marquéz de la Rubia, Francisco, *op. cit.*

ha sido uno de los desarrollos más valiosos de la cooperación de inteligencia occidental, y su dilución representaría una pérdida colectiva de conocimiento operativo difícilmente recuperable.

El caso iraní, finalmente, añade una dimensión que trasciende el conflicto bilateral. Los ataques a infraestructura estadounidense no son únicamente actos de coerción, son señales geopolíticas codificadas, dirigidas simultáneamente a Israel, a los aliados regionales de Washington y a la opinión pública interna iraní. En ese lenguaje de señales estratégicas, la respuesta cibernética de Estados Unidos (o su ausencia) es leída como indicador de credibilidad y resolución que afecta percepciones de poder en escenarios que van mucho más allá del dominio digital.[58]

Chile ante el espejo: lecciones estratégicas para una potencia media en el ciberespacio

Analizar la ciberdefensa estadounidense exclusivamente desde una perspectiva interna sería, para las naciones latinoamericanas, un ejercicio de contemplación estética. La relevancia del caso radica precisamente en su capacidad de iluminar vulnerabilidades, patrones de amenaza y dilemas de gobernanza que, con las proporciones ajustadas, reproducen las condiciones que enfrentan países de mediano desarrollo tecnológico como Chile. Ignorar esas lecciones sería un lujo que la trayectoria del conflicto cibernético global ya no permite.

Chile ocupa en el ciberespacio latinoamericano una posición ambivalente: es simultáneamente uno de los países más digitalizados de la región y uno de los más expuestos. Con una economía cuyos sectores estratégicos (minería, energía, servicios financieros, telecomunicaciones y transporte) dependen crecientemente de infraestructura digital conectada y con sistemas de control industrial (ICS[59]/OT) que exhiben niveles de exposición documentados por la OEA[60] y el BID[61] Chile presenta un perfil de vulnerabilidad estructuralmente análogo al que el CISA ha identificado en instalaciones estadounidenses atacadas por actores iraníes: sistemas de control conectados a internet con credenciales insuficientes o con patrones de segmentación de red inadecuados.

El avance legislativo más significativo de los últimos años ha sido la promulgación de la Ley N.° 21.663, Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, publicada el 8 de marzo

58 Industrial Cyber. CSIS flags Iran's shift from episodic cyberattacks to sustained campaign against critical infrastructure. 9 de abril de 2026, [En línea]. Disponible en: https://industrialcyber.co/industrial-cyber-attacks/csis-flags-irans-shift-from-episodic-cyberattacks-to-sustained-campaign-against-critical-infrastructure/

59 ICS (Industrial Control Systems): sistemas utilizados para supervisar, monitorear y controlar procesos industriales y de automatización mediante dispositivos electrónicos, redes y software especializado.

60 OEA (Organización de los Estados Americanos): organismo internacional que reúne a los países del continente americano con el propósito de promover la cooperación, la democracia, la seguridad, los derechos humanos y el desarrollo integral entre los Estados miembros.

61 Organización de los Estados Americanos (OEA) / Banco Interamericano de Desarrollo (BID). (2020). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington D.C.: OEA/BID

de 2024.[62] Esta ley crea la Agencia Nacional de Ciberseguridad (ANCI[63]), establece un catálogo de infraestructuras críticas de la información, fija obligaciones de notificación de incidentes para operadores de sectores esenciales y articula un modelo de coordinación intersectorial que tiene como referente explícito las arquitecturas de gobernanza cibernética de países OCDE.

El CSIRT[64] Nacional, adscrito al Ministerio del Interior y Seguridad Pública, opera como nodo de respuesta técnica y alerta temprana . A partir de la experiencia estadounidense analizada, resulta pertinente considerar que la efectividad de una arquitectura nacional de ciberseguridad no depende exclusivamente de su marco normativo, sino también de la existencia de capacidades técnicas especializadas, recursos adecuados y procesos sostenidos de fortalecimiento institucional. Estas condiciones constituyen elementos relevantes para interpretar los desafíos asociados a la implementación de la nueva institucionalidad chilena, especialmente en un escenario caracterizado por la creciente sofisticación y dinamismo de las amenazas cibernéticas.

El análisis del caso estadounidense ofrece a Chile cinco lecciones de aplicación directa:

La primera es que la reducción presupuestaria en ciberdefensa nunca es neutral: la experiencia de la CISA en 2026, debilitada precisamente cuando la amenaza iraní alcanzaba su mayor intensidad, ilustra con dramática claridad que las brechas de capacidad defensiva no esperan a que el presupuesto se recupere. Para la ANCI chilena, esto implica que el proceso de dotación de capacidades debe estar protegido de las fluctuaciones del ciclo político-electoral.

La segunda lección es que la infraestructura crítica es tan débil como su eslabón más expuesto: los ataques iraníes contra instalaciones de agua estadounidenses no explotaron vulnerabilidades sofisticadas, sino contraseñas predeterminadas y conexiones a internet sin segmentación. En Chile, donde el sector minero y el sistema de gestión de aguas operan con tecnología OT[65] de generaciones diversas, la prioridad inmediata debería ser un inventario sistemático de exposición y un programa acelerado de higiene cibernética básica.

La tercera lección es que la dependencia tecnológica de un único proveedor es una vulnerabilidad estratégica: el debate sobre el contexto del DoD estadounidense tiene un equivalente estructural para Chile en la concentración de infraestructura digital crítica en plataformas extranjeras sin requisitos de transferencia tecnológica, auditoría independiente o protocolos de contingencia nacional.

La cuarta lección es que la coordinación público-privada no es opcional. Dado que la

62 Ministerio del Interior y Seguridad Pública de Chile. Ley N.° 21.663 Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Santiago: Diario Oficial de la República de Chile. 2024.

63 Agencia Nacional de Ciberseguridad (ANCI): organismo encargado de coordinar, fortalecer y supervisar las políticas, estrategias y acciones relacionadas con la ciberseguridad a nivel nacional, con el objetivo de proteger las infraestructuras digitales, los sistemas informáticos y la información crítica frente a amenazas y ciberataques.

64 Computer Security Incident Response Team (CSIRT): grupo especializado encargado de detectar, analizar, gestionar y responder a incidentes de ciberseguridad, con el objetivo de minimizar impactos, restaurar sistemas afectados y fortalecer la protección de las infraestructuras digitales.

65 La Tecnología de Operaciones (OT) comprende el hardware y software especializado que monitoriza y controla dispositivos físicos en plantas industriales, redes de energía o infraestructuras críticas.

mayor parte de la infraestructura crítica chilena (energía, telecomunicaciones, servicios financieros y transporte) es de propiedad privada, la ANCI no puede operar como una agencia de defensa estatal clásica: requiere mecanismos de intercambio de inteligencia de amenazas, protocolos de notificación y respuesta conjunta, e incentivos regulatorios que alineen los intereses comerciales con los objetivos de seguridad nacional.

La quinta lección, y quizás la más compleja de incorporar, es que la IA en ciberdefensa exige gobernanza antes que despliegue. La apresurada integración de Grok en el ecosistema de defensa estadounidense, sin marcos de auditoría, sin protección de datos de los servidores militares y sin resolución de los conflictos de interés del proveedor, ilustra los riesgos de priorizar la velocidad de adopción por sobre la solidez del marco de gobernanza.

Para Chile, cuya ANCI está en proceso de diseñar su arquitectura de capacidades, existe una ventana de oportunidad para construir desde el inicio un modelo de integración de IA en ciberdefensa que incluya supervisión humana en los puntos de decisión críticos, mecanismos de transparencia algorítmica y requisitos de localización o auditoría de datos de naturaleza sensible.

La tabla N.°2 resume los principales vectores de amenaza analizados en el artículo y sus implicancias específicas para el contexto chileno:

Vector de amenaza	Implicancia para Chile
Actores estatales de capacidad media (tipo IRGC).	Alta exposición de infraestructuras OT/ICS en energía, agua y minería con credenciales débiles. Patrón análogo al detectado por CISA en EE.UU.
IA aplicada al ciberataque (deepfakes, phishing adaptativo).	Ausencia de capacidades nacionales de detección basada en IA; dependencia de soluciones comerciales extranjeras sin adaptación al contexto institucional chileno.
Dependencia de plataformas tecnológicas extranjeras	Riesgo soberano al adoptar LLM[66] de proveedores únicos para funciones sensibles del Estado sin marco de gobernanza de datos asociado.
Fragmentación de la gobernanza cibernética.	La reciente Ley N.° 21.663 crea la ANCI, pero la coordinación intersectorial y la articulación con Fuerzas Armadas aún están en etapa de implementación.
Geopolítica hemisférica (NSS-2025 Monroe / Trump)	Chile, como socio preferencial de EE.UU. puede acceder a inteligencia de amenazas y cooperación técnica, pero también absorbe las tensiones del repliegue multilateral estadounidense.

Tabla N.°2: Vectores de amenaza cibernética y sus implicancias para Chile.

Fuente: Elaboración propia.

Chile posee, en suma, activos estratégicos que justifican una política de ciberdefensa robusta y sostenida: infraestructura energética y minera de importancia hemisférica, posición geográfica que la hace nodo de cables submarinos de comunicaciones, rol de país OCDE que amplifica

66 LLM (Large Language Model o Modelo de Lenguaje de Gran Escala) es un sistema de inteligencia artificial entrenado con grandes cantidades de texto para comprender, generar y procesar lenguaje natural. Estos modelos utilizan redes neuronales avanzadas para responder preguntas, redactar textos, traducir idiomas, programar y realizar diversas tareas relacionadas con el lenguaje humano.

su exposición a actores de amenaza estatales y no estatales, y una trayectoria de integración en redes de inteligencia y cooperación de seguridad con socios de alto estándar tecnológico.

La NSS-2025, con su énfasis en el hemisferio occidental como esfera de influencia preferente, abre paradójicamente espacios de cooperación reforzada en ciberinteligencia y estándares de defensa que Chile debería aprovechar con criterio estratégico, sin sacrificar la diversificación de sus relaciones de seguridad ni la soberanía sobre sus datos e infraestructuras más sensibles.

Reflexiones finales

El análisis desarrollado en las páginas precedentes permite articular tres conclusiones de orden estratégico que, leídas en conjunto, trazan el perfil de un cambio de época cuyas consecuencias apenas estamos comenzando a dimensionar.

La primera conclusión es que la ciberseguridad ha completado su transición desde el dominio técnico subsidiario hasta un eje estructurante de la competencia entre potencias. La divergencia doctrinal entre la NSS-2022 de Biden y la NSS-2025 de Trump no expresa únicamente una diferencia de partido; refleja una disputa más profunda sobre la ontología misma del ciberespacio: ¿es un bien público global que los Estados deben contribuir a gobernar colectivamente, o es un dominio de ventaja competitiva que cada potencia debe colonizar en beneficio propio? La respuesta a esta pregunta no es neutral para el sistema internacional: si la segunda visión prevalece y se generaliza –como el comportamiento de actores como China y Rusia sugiere que ya está ocurriendo–, la fragmentación del ecosistema digital global en bloques de soberanía tecnológica incompatible podría producir un *cyber Iron Curtain* con consecuencias para la estabilidad del orden internacional comparables a las de la división de la posguerra fría.

La segunda conclusión es que la amenaza asimétrica iraní ha demostrado la insostenibilidad del modelo de ciberdefensa reactiva. Irán no necesita equipararse tecnológicamente a Estados Unidos para causar daño estratégico; le basta con la sistematicidad, la explotación de vectores de baja tecnología (contraseñas predeterminadas, dispositivos OT obsoletos, redes sin segmentación) y la disposición a escalar cuando la respuesta del adversario es percibida como contenida. La reducción de capacidades de la CISA en el momento de mayor presión operativa no es únicamente una paradoja presupuestaria; es el indicador más preocupante de una brecha entre la narrativa de supremacía tecnológica de la NSS-2025 y la realidad operativa de la defensa del territorio nacional.

La tercera conclusión atañe a la inteligencia artificial en ciberdefensa y es, por sus implicancias de largo alcance, la más urgente. La integración acelerada de LLM en los sistemas de defensa del Pentágono (con los casos *Grok/GenAI.mil* como expresión emblemática) refleja una decisión estratégica correcta en su dirección, pero prematura en su arquitectura de gobernanza. La IA puede transformar radicalmente la capacidad defensiva de cualquier actor; pero desplegada sin supervisión humana robusta, sin marcos de auditoría independiente y sin resolución de los conflictos de interés que genera la dependencia de proveedores privados, puede convertirse en el vector de vulnerabilidad más peligroso que el sistema de defensa nacional haya incorporado en su historia reciente. La velocidad no es una virtud en sí misma cuando los errores del algoritmo se propagan a la velocidad de la luz.

Para Chile y para los países latinoamericanos que observan estos desarrollos desde la periferia tecnológica del sistema internacional, la lección transversal es que la ciberdefensa del siglo XXI no admite postergación. No porque las amenazas sean inminentes en términos idénticos a los que enfrenta Estados Unidos, sino porque las ventanas de construcción institucional y de capacidad técnica se cierran con la misma rapidez con que evoluciona el panorama de amenazas.

Invertir hoy en la maduración de la ANCI, en la higiene cibernética de la infraestructura crítica, en la formación de talento especializado y en marcos de cooperación internacional bien calibrados es, en términos de relación costo-beneficio estratégico, infinitamente más eficiente que responder a una crisis cuando ya se ha producido.

Entonces, la pregunta ¿puede la disuasión trasladarse con eficacia al dominio cibernético?, no tiene una respuesta binaria. Lo que el análisis sugiere es que la disuasión en el ciberespacio es posible, pero requiere ser reinventada: no como la amenaza de destrucción mutua asegurada que disciplinó la Guerra Fría nuclear, sino como la combinación de resiliencia demostrada, capacidad de respuesta proporcional y comunicación estratégica calibrada que convierte al ciberataque en un instrumento de rendimientos decrecientes para quien lo emplee. Construir esa arquitectura ya sea en Washington, en Santiago o en cualquier capital que aspire a defender su soberanía digital, es el desafío definitorio de la política de seguridad nacional en las próximas décadas.

Bibliografía

ABC NEWS. DHS shutdown fuels cybersecurity concerns as Iran-linked cyberattacks continue across US. 3 de abril de 2026, [En línea]. Disponible en: https://abcnews.com/Politics/dhs-shutdown-fuels-cybersecurity-concerns-iran-linked-cyberattacks/story?id=131546421

BIDEN, Joseph. National Cybersecurity Strategy. Washington D.C.: White House Office of the National Cyber Director. 2 de marzo de 2023, [En línea]. Disponible en: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS). Iran Conflict Heightens Cyber Threats to U.S. Energy Infrastructure. 9 de abril de 2026, [en línea]. Disponible en: https://www.csis.org/analysis/iran-conflict-heightens-cyber-threats-us-energy-infrastructure

COKER, Harry Jr. Annual Report on the United States Cybersecurity Posture. Washington D.C.: Office of the National Cyber Director. 2024. [En línea]. Disponible en: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

CSIRT Nacional de Chile. Informe de Tendencias en Ciberseguridad 2024. Santiago: Ministerio del Interior y Seguridad Pública. 2024, [En línea]. Disponible en: https://www.csirt.gob.cl

CSO ONLINE. How the US DOD Cyber Strategy changes national cyber defense. 2024, [En línea]. Disponible en: https://www.csoonline.com/article/655937/how-the-us-dod-cyber-strategy-changes-national-cyber-defense.html

CYBERSECURITY AND INFRASTRUCTURE SECU-

RITY AGENCY (CISA), FEDERAL BUREAU OF INVESTIGATION (FBI), DC3. Joint Cybersecurity Advisory AA24-241A: Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations. Agosto 2024, [En línea]. Disponible en: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), FEDERAL BUREAU OF INVESTIGATION (FBI), NATIONAL SECURITY AGENCY (NSA). Updated Advisory AA23-335A: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities. 18 de diciembre de 2024, [En línea]. Disponible en: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest. 30 de junio de 2025, [En línea]. Disponible en: https://www.ic3.gov/CSA/2025/250630.pdf

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). Iran Threat Overview and Advisories. Cybersecurity and Infrastructure Security Agency. 2024, [En línea]. Disponible en: https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran

DEFENSESCOOP. Sen. Warren letter to Hegseth on Musk-xAI DoD Contract. 11 de septiembre de 2025, [En línea]. Disponible en: https://defensescoop.com/2025/09/11/sen-warren-letter-hegseth-musk-xai-dod-contract/

DoD CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICE (CDAO). CDAO Announces Partnerships with Frontier AI Companies to Address Critical National Security Challenges. Defense News. Junio 2025, [En línea]. Disponible en: https://www.defensenews.com/pentagon/2025/07/15/pentagon-taps-four-commercial-tech-firms-to-expand-military-use-of-ai/

DOD CYBER STRATEGY 2023 SUMMARY. U.S. Department of Defense. 12 de septiembre de 2023, [En línea]. Disponible en: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

FOUNDATION FOR DEFENSE OF DEMOCRACIES (FDD). How an Iranian Cyberattack Hit US Local Governments. 14 de abril de 2026, [En línea]. Disponible en: https://www.fdd.org/analysis/2026/04/14/how-an-iranian-cyberattack-hit-us-local-governments/

FRÍAS Sánchez, Carlos Javier. El campo de batalla futuro… que quizá es presente. Madrid: Instituto Español de Estudios Estratégicos, Documento Marco 07/2021. 19 de mayo de 2021, [En línea]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM07_2021_CARFRI_Batalla.pdf

GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED, 22 de agosto de 2018, [En línea]. Disponible en: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

INDUSTRIAL CYBER. CSIS flags Iran's shift from

episodic cyberattacks to sustained campaign against critical infrastructure. 9 de abril de 2024, [En línea]. Disponible en: https://industrialcyber.co/industrial-cyber-attacks/csis-flags-irans-shift-from-episodic-cyberattacks-to-sustained-campaign-against-critical-infrastructure/

KELLO, Lucas. The Virtual Weapon and International Order. New Haven: Yale University Press. 22 de agosto de 2017, [En línea]. Disponible en: https://www.academia.edu/61597942/The_Virtual_Weapon_and_International_Order

KLIMBURG, Alexander. The Darkening Web: The War for Cyberspace. New York: Penguin Press. p. 58.

MÁRQUEZ DE LA RUBIA, Francisco. La Estrategia de Seguridad Nacional de los Estados Unidos (2025): análisis y comparativa con la ESN 2022. IEEE-CESEDEN. 10 de diciembre de 2025, [En línea]. Disponible en: https://www.defensa.gob.es/ceseden/-/ieee/la-estrategia-seguridad-nacional-de-estados-unidos

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA DE CHILE. Ley N.° 21.663 Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Santiago: Diario Oficial de la República de Chile. 2024.

NATIONAL SECURITY AGENCY (nsa) / Central Security Service (css). 2023 NSA Cybersecurity Year in Review. Fort Meade, MD: NSA.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA) / BANCO INTERAMERICANO DE DESARROLLO (BID). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington D.C.: OEA/BID. 2020.

PEISER, Jaclyn. A hacker tried to poison the water supply in Oldsmar, Florida, police said. The Washington Post. 9 de febrero de 2021, [En línea]. Disponible en: https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/

PERLROTH, Nicole. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, The New York Times. 23 de octubre de 2012, [En línea]. Disponible en: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

RID, Thomas. Cyber War Will Not Take Place. Oxford: Oxford University Press. 2013.

SATNEWS. The Pentagon's Faustian Bargain: Buying Speed, Building a Monopoly. 24 de diciembre de 2025, [En línea]. Disponible en: https://news.satnews.com/2025/12/24/the-pentagons-faustian-bargain-buying-speed-building-a-monopoly/

U.S. CYBER COMMAND. Persistent Engagement and Defending Forward. Fort Meade, MD: CYBERCOM. 2023.

U.S. DEPARTMENT OF JUSTICE, United States v. Ahmad Fathi *et al.*, Indictment, S.D.N.Y., 24 de marzo de 2016, pp. 4–7, [En línea]. Disponible en: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

U.S. DEPARTMENT OF WAR. (2025, 22 de diciembre). The War Department to Expand AI Arsenal on GenAI.mil With xAI. [En línea]. Disponible

en: https://www.war.gov/News/Releases/Release/Article/4366573/

VEGO, Milan. RECCE-Strike Complexes in Soviet Theory and Practice. Fort Leavenworth, KS: Soviet Army Studies Office. Junio de 1990, [En línea]. Disponible en: https://apps.dtic.mil/sti/pdfs/ADA231900.pdf

WARREN, Elizabeth. Letter to Secretary Hegseth Regarding Integration of Grok into DoD Operations. U.S. Senate. 10 de septiembre de 2025, [En línea]. Disponible en: https://www.warren.senate.gov/imo/media/doc/letter_to_pentagon_regarding_integration_of_grok_91025.pdf

xAI. xAI for Government: US Department of War Partnership. Diciembre 2025, [En línea]. Disponible en: https://x.ai/news/us-gov-dept-of-war