Análisis comparativo de las estrategias de Ciberdefensa del Ejército de los Estados Unidos y Rusia: implicaciones para la seguridad nacional

Mayor (EJC) José Antonio Calderón Arias

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) José Antonio Calderón Arias
Identificación	**:**	1026251824
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Coronel Aldemar Serrano Cuervo
Tutor temático	**:**	Angelica María González González
Fecha de entrega	**:**	26 de agosto de 2025
Extensión	**:**	10.837 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Análisis comparativo de las estrategias de Ciberdefensa del Ejército de los Estados Unidos y Rusia: implicaciones para la seguridad nacional

Comparative analysis of US and Russian Army cyber-defense strategies: implications for national security

José Antonio Calderón Arias [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente artículo busca analizar cuál de las estrategias de Ciberdefensa en los países de Estados Unidos y Rusia, ha resultado tener mayor efectividad para la respuesta frente a incidentes cibernéticos. Se uso una metodología cualitativa con un diseño descriptivo-analítico, en el que se contempló investigaciones previas, normatividad e informes militares. Los hallazgos indican que Colombia ha trabajado en robustecer su capacidad de Ciberdefensa, sin embargo, el trabajo es arduo y los desafíos son indeterminados por llegar a una protección total en relación a las tácticas, estrategias y tecnología que posee otros países. El estudio sugiere que la mejora de tecnología, una adecuada planeación, creación y ejecución de políticas permitirían un panorama diferente a nivel mundial de Colombia; siendo pilar fundamental el fortalecimiento de la capacidad operativa de las Fuerzas Militares. Finalmente, la comparación con sistemas de estrategias de Ciberdefensa del Ejercito de los Estados Unidos y Rusia, arroja un modelo hibrido de defensa y mejoramiento de la ciberdefensa de Colombia.

Palabras clave: Tecnología de información; Defensa Militar; Capacidad Tecnológica; Seguridad Datos.

Abstract: This article aims to analyze which of the Cyber Defense strategies in the United States and Russia has proven to be most effective for responding to cyber incidents. A qualitative methodology with a descriptive-analytical design was used, in which previous investigations, norms and military reports were considered. The findings indicate that Colombia has worked to strengthen its Cyber Defense capacity, however, the work is arduous and the challenges are undetermined to reach a total protection in relation to the tactics, strategies and technology that other countries possess. The study suggests that the improvement of technology, proper planning, creation and implementation of policies would allow a different picture at the global level of Colombia; being fundamental pillar strengthening the operational capacity of the Military Forces. Finally, the comparison with US and Russian Army cyber-defense strategy systems produces a hybrid model of defense and improvement of Colombia's cyber-defense.

Keywords: Information Technology; Military Defense; Technological Capability; Data Security.

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: jose.calderon@esdeg.edu.co.

Introducción

La Ciberdefensa es el incorporado de pericias, políticas y procesos técnicos delineados para resguardar las estructuras de datos, redes y aparatos contra ofensivas cibernéticas. Se enfoca en la prevención, rastreo y refutación a amenazas, con la finalidad de empequeñecer el impacto y preservar la integridad de los sistemas. El avance de la Ciberdefensa ha sido un tema central en la seguridad nacional de potencias como Estados Unidos y Rusia, dos países con enfoques distintos en la protección de sus activos digitales y militares. Por esta razón "el progreso de las estrategias de ciberseguridad ha sido promovida por el progresivo refinamiento de los ataques cibernéticos, lo que ha conducido a la implementación de estructura de defensa más resistentes" (Hassan, Haroon, Khalid, Ghayoor, 2024, p. 3).

Del mismo modo, Colombia afronta dificultades estructurales significativas en el desarrollo e implementación de una estrategia integral de ciberdefensa, debido principalmente a la inexistencia de una doctrina unificada y a la fragmentación de competencias entre varias entidades gubernamentales. Esta fragmentación institucional limita la eficacia del país para anticipar, prevenir y responder de manera articulada a las amenazas en el ciberespacio. En este contexto, el análisis comparativo de las estrategias de ciberdefensa de Estados Unidos y Rusia resulta decisiva, ya que permite precisar tanto sus fortalezas como sus debilidades, y recoger enseñanzas estratégicas que puedan ser adaptadas y ejecutadas al caso colombiano, con miras a reforzar sus capacidades nacionales relativas a la ciberseguridad (Díaz y Cremades, 2024).

Cabe señalar también que, la ciberseguridad en el ámbito militar ha evolucionado como un dominio clave en la defensa nacional, con Estados Unidos y Rusia liderando estrategias distintas. De acuerdo con Seitz, 2024, Estados Unidos prioriza un enfoque preventivo y de cooperación con el sector privado, mientras que Rusia integra la ciberguerra en su actuar ofensivo demostrando fortalezas y vulnerabilidades en la protección de infraestructuras críticas. La comparación de estas estrategias permite evaluar su efectividad y extraer lecciones para fortalecer la Ciberdefensa en Colombia, adaptando medidas exitosas a su contexto de seguridad nacional.

Así mismo, ambos modelos han sido probados en incidentes cibernéticos recientes, por el lado de Estados Unidos, en el mes de abril (2025) tuvo dos ataques cibernéticos: 1). "Hackers espiaron los correos electrónicos cerca de 103 reguladores bancarios estadounidenses de la Oficina del Contralor de la Moneda durante más de un año" y 2). el Comando Cibernético de Estados Unidos reveló malware chino instaurado en redes agrupadas de varias naciones latinoamericanas durante una cadena de operaciones de "búsqueda anticipada" (CSIS, 2025). Mientras que Rusia en el mes de abril del año 2024, recibió un ciberataque de "la agencia de inteligencia militar de Ucrania contra su partido gobernante. Los atacantes lanzaron una andanada de ataques DDoS contra los servidores, sitios web y dominios de Rusia Unida para inaccesibles" (CSIS, 2025).

En consecuencia, este estudio busca alcanzar el siguiente objetivo general: analizar las estrategias de Ciberdefensa implementadas por los Ejércitos de Estados Unidos y Rusia, evaluando efectividad, los enfoques adoptados, las capacidades de respuesta ante incidentes cibernéticos y las implicaciones para la seguridad nacional de cada país. Y los objetivos

específicos: 1) identificar las capacidades tecnológicas y tácticas de Ciberdefensa empleadas por los ejércitos de Estados Unidos y Rusia para la protección de sus activos militares y gubernamentales; 2) Comparar las políticas nacionales de Ciberdefensa de cada país, evaluando las estrategias de prevención, detección y respuesta ante ciberataques, y cómo estas políticas se integran dentro de sus doctrinas de defensa militar; 3) investigar los incidentes cibernéticos más relevantes en los que Estados Unidos y Rusia han estado involucrados, y analizar cómo sus respectivas estrategias de Ciberdefensa han influido en la protección de sus infraestructuras críticas y en la respuesta ante ciberamenazas y 4) identificar fortalezas de las comparaciones para aplicarlas en Colombia.

Pregunta de investigación: ¿Qué aporte brinda las estrategias de Ciberdefensa de los países de Estados Unidos y Rusia, para una efectiva y actualizada protección de la ciberseguridad en Colombia?

Metodología

La investigación adopta un enfoque cualitativo, orientado a comprender en profundidad las estrategias de Ciberdefensa implementadas por Estados Unidos y Rusia, evaluando su efectividad y sus implicaciones en la seguridad nacional. Este enfoque permite analizar documentos y estudios de casos relevantes, facilitando la identificación de similitudes, diferencias y oportunidades de mejora en el contexto colombiano. Al centrarse en la interpretación de la información disponible, el estudio ofrecerá una visión integral sobre cómo estos países han desarrollado sus capacidades de Ciberdefensa y cómo pueden servir de referencia para fortalecer la estrategia colombiana (Urbina, 2020).

El diseño de la investigación es descriptivo-analítico, ya que busca describir y comparar los enfoques de Ciberdefensa de Estados Unidos y Rusia. A través del análisis documental, se examinaron normativas, doctrinas militares, informes gubernamentales y literatura académica, con el fin de establecer un diagnóstico detallado sobre la efectividad de sus estrategias y las lecciones aplicables al contexto colombiano (Angarita y Díaz, 2020). Este enfoque permitirá no solo describir las estrategias implementadas, sino también extraer conclusiones basadas en la revisión de experiencias internacionales.

Se planteo una fase inicial de revisión documental, en la que la selección estará compuesta por documentos clave sobre políticas y estrategias de Ciberdefensa en Estados Unidos y Rusia. Se incluirán normativas nacionales de cada país, informes de organismos de seguridad, estudios académicos y reportes sobre ciberataques relevantes en los que estos países han estado involucrados. Estos documentos proporcionarán información fundamental para evaluar la efectividad de sus estrategias de ciberseguridad y cómo estas han influido en su capacidad de respuesta ante incidentes cibernéticos.

La revisión documental se efectuó en dos revistas, la primera es de la escuela superior de guerra "General Rafael Reyes Prieto" y la segunda es la revista de estudios en Seguridad y defensa como también bibliotecas electrónicas como Scielo, Redalyc y Dialnet. Seleccionando documentos e investigaciones previas no mayor a 5 años de tal forma que, aporten datos relevantes, actualizados y aplicables a los objetivos de la investigación. La selección se basará en criterios como la actualidad, la aplicabilidad al ámbito militar y la relación directa con las estrategias de Ciberdefensa en cada país. Este tipo de estudio

garantiza que la información obtenida sea pertinente y permita generar resultados significativos (Ortega, 2023).

El instrumento principal para la recopilación de datos será una matriz de análisis documental, que permitirá organizar la información obtenida, facilitando la identificación de patrones, estrategias y tendencias clave en Ciberdefensa. A través de esta herramienta, será posible sistematizar los hallazgos y generar un análisis más estructurado, alineado con los objetivos de la investigación.

Se establecieron criterios específicos para la selección de las fuentes de información. Los criterios de inclusión considerarán documentos oficiales de defensa de Estados Unidos y Rusia, normativas, informes técnicos y estudios de casos internacionales sobre ciberseguridad militar. También se incluyeron artículos académicos recientes (últimos 5 años) que aporten perspectivas relevantes al tema. Los criterios de exclusión abarcarán documentos obsoletos, fuentes no verificables o aquellas que no se relacionen directamente con la Ciberdefensa en el contexto militar. Esto asegurará que la información utilizada sea precisa y pertinente para los fines del estudio.

Ciberespacio y su Impacto en la Defensa Nacional

En las últimas décadas, la innovación digital ha afianzado al ciberespacio como un nuevo dominio estratégico en el que convergen sistemas de información, redes de comunicación, infraestructuras críticas y usuarios interconectados globalmente. En oposición de los espacios físico-terrestres tradicionales, el ciberespacio se especifica por su ambiente

intangible, transnacional y dinámicamente progresiva, lo cual simboliza tanto una oportunidad como un reto para la soberanía y la seguridad de los Estados (Rodríguez, 2022).

En este contexto, la defensa nacional ha precisado acomodarse a las razones del entorno digital, reconociendo que los conflictos presentes, ya no se desenvuelven únicamente en campos de batalla físicos, sino también en escenarios cibernéticos donde se extienden operaciones ofensivas y defensivas que envuelven la persistencia institucional, la integridad de las infraestructuras estratégicas y la gobernanza digital (Niss, 2023). Así, los ataques cibernéticos a servicios fundamentales, como los sistemas eléctricos, financieros, salubres o de comunicaciones estatales, se han transformado en una amenaza real para la seguridad nacional.

Asimismo, es importante recalcar que el ciberespacio ha sido explícitamente reconocido por organismos multilaterales, como la OTAN y la Unión Europea, como un dominio operativo autónomo, lo que involucra que las capacidades de ciberdefensa se traten del mismo modo que las de defensa terrestre, aérea, marítima o espacial (NATO, 2024). Esta idea exige a los Estados a desarrollar doctrinas específicas, marcos legales adaptativos, alianzas estratégicas internacionales y estructuras institucionales diligentes a la vigilancia, respuesta y disuasión en el ciber ámbito.

En consecuencia, el impacto del ciberespacio en la defensa nacional no solo es técnico, sino también geopolítico, jurídico y ético, ya que traza nuevos interrogantes sobre la atribución de ataques, la proporción en la refutación y la delimitación entre actos de guerra y actos de cibercrimen (Expósito, 2021). Frente a ello, la integración de políticas públicas de

ciberseguridad, educación digital y cooperación internacional forma una condición vital para certificar la resiliencia de las democracias ante las amenazas emergentes del siglo XXI.

Es importante, continuar por detallar levemente los conceptos de ciberseguridad y ciberdefensa para ahondar en la investigación. Así que, la ciberseguridad se ha convertido en una prioridad para los gobiernos de todo el mundo, ya que discurren que preservar los bienes aprovechables a través de internet, los procedimientos y las redes informáticas de los hackers, es transcendental para la marcha, la persistencia de un país y el sostén de su ciudadanía. Los principales ataques cibernéticos consiguiendo los 1.308 en el primer trimestre de 2024 (Secureframe, 2024), son contra servicios públicos, datos y redes implicadas; por eso los mercados y los habitantes exploran la escasez de tomar medidas.

Por otro lado, la Ciberdefensa es la fusión de acciones y reglas efectuadas por un país para proteger los datos, los sistemas y las redes de ataques cibernéticos (Rodríguez, 2022), y cuenta con dos enfoques: Ciberdefensa defensiva y Ciberdefensa ofensiva; mientras que, la ciberseguridad, de acuerdo con el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), es el conjunto de habilidades y métodos diseñados para proteger sistemas informáticos y de comunicación frente a amenazas internas o externas (National Institute of Standards and Technology, 2024).

Ciberdefensa

Las estrategias de Ciberdefensa han evolucionado en respuesta a las amenazas emergentes en el ciberespacio, en donde las campañas de manipulación social y los ataques cibernéticos se han convertido en herramientas claves dentro de la guerra híbrida. Destaca Martin (2022) que el ciberespacio se ha transformado en un campo de batalla donde actores

estatales y no estatales, implementan estrategias de desinformación y ciberataques para afectar la estabilidad política y la seguridad nacional. También, el desarrollo de la Ciberdefensa ha sido impulsado por la evolución del ciberterrorismo, el cual se ha convertido en una amenaza híbrida que desafía la seguridad nacional de múltiples Estados.

Ciberdefensa como Concepto

Desde una vista conceptual, la ciberdefensa se puede explicar como el conjunto de principios, experiencias, tecnologías y técnicas encaminadas a resguardar sistemas, redes y datos digitales ante amenazas, ofensiva o actividades hostiles en el ciberespacio (Mogollón, 2021). Esta dirección encierra la defensa tanto reactiva como proactiva delante de acciones malintencionadas que logren complicar la confidencialidad, moralidad o acceso de los datos.

En este sentido, la ciberdefensa se dispone como una creación teórica multifacética, en la que convergen especialidades como la criptografía, la inteligencia artificial, la seguridad informática, la ingeniería de software, el derecho internacional y las políticas públicas.

Autores como Nobrega, Rutkowski y Saunders (2024) recalcan que la ciberdefensa no debe llegar hasta una vacía técnica a sucesos, sino que también envuelve una razón política y estratégica del ciberespacio como una potestad más de la defensa nacional, al mismo nivel que la tierra, el mar, el aire y el espacio.

Ciberdefensa como Estrategia

Cuando se encara la ciberdefensa como estrategia, se hace alusión de la proyección, organización y cumplimiento de acciones ordenadas para advertir, descubrir, responder y rescatar amenazas en el ciberespacio, en la perspectiva de una enfoque geopolítico o institucional específico (Agencias Externas, 2024).

Desde esta vista, la ciberdefensa estratégica se modifica hacia una función operacional del Estado, las fuerzas armadas o las organizaciones críticas, y puede entrar a ser parte de doctrinas militares o de seguridad nacional, por ejemplo, la estrategia de Ciberdefensa de la OTAN (NATO, 2024) instaura lineamientos claros para integrar el ciberespacio dentro de sus operaciones defensivas, reconociéndolo como un dominio operacional y prevaleciendo el desarrollo de saberes para la resiliencia cibernética.

Ciberdefensa Defensiva y Ciberdefensa Ofensiva

La ciberdefensa defensiva es la principal vía de protección contra los ciberataques, esta se compone de: medidas preventivas, análisis reiterados del sistema y refutación a sucesos en tiempo real para crear ciberresiliencia y resguardar sus activos. Este contexto no es inquebrantable, exigiendo la actuación inmediata y eficaz para finalizar con la amenaza y aminorar los perjuicios, retornando a la normalidad lo antes posible (Expósito, 2021).

Mientras que, la ciberdefensa ofensiva es poner en marcha toda la planeación junto con las herramientas previas ejecutadas en la ciberdefensa defensiva. Incluyendo las tácticas y métodos frente al agresor que atenta contra el país u organización. No toda vez, se ejecutan para dañar a otros, sino para perfeccionar la seguridad de una organización (Niss, 2023).

Por otro lado, y de acuerdo con Rivera y Hernández, 2023, la guerra híbrida inicia en amenazas híbridas, las cuales son operaciones ordenadas y concordadas que atacan las debilidades corporativas de los Estados y sus instituciones de manera premeditada por medio de una diversidad de formas y en múltiples sectores como: estatales, financieros, ejércitos, sociales, periodísticos, infraestructuras y legales) usando el ciberespacio como instrumento.

Según Verdugo, 2020, el conflicto híbrido es el escenario en el que las partes se limitan al uso directo de la fuerza armada y operan combinando la amenaza militar (sin llegar a un ataque tradicional) y al aprovechamiento de debilidades bancarias, gubernativas, técnicas y diplomáticas.

El ciberespacio como nuevo campo de batalla

Avances tecnológicos: La tecnología en la actualidad es una necesidad más que un gusto por aprenderla. Todo está comunicado y muchas organizaciones se esfuerzan por elevar sus procesos a espacios virtuales que expandan sus actividades económicas como el alcance a un mayor número de clientes; y después de la pandemia se evidencio la magnitud y la importancia que la tecnología genera en el desarrollo de un país. Esto se expande y cada vez se requiere de un mayor conocimiento para abarcar las emergencias que las necesidades generan Los avances tecnológicos han permitido la creación de nuevos escenarios de combate en el ciberespacio. Las múltiples tareas que a diario se realizan en las organizaciones y el diario vivir son: el uso de internet, las redes sociales, email y mensajería momentánea, video llamadas, inteligencia artificial, análisis de datos, transformación a la economía, etc. (Brodowicz, 2024).

Uso en la guerra: El ciberespacio es el nuevo auge, para intimidar al enemigo. Los Estados y sus ejércitos ven en el ciberespacio la nueva oportunidad para acobardar la seguridad nacional de otro país y medio de ataque; ya que, aquel que no tenga armamento y seguridad en su espacio virtual puede ser blanco fácil para otros, atentando con su infraestructura (Arias y Manzano, 2023).

Conflicto internacional: El ciberespacio muestra una nueva situación de conflicto mundial en la que se ha desbordado sin remediar ningún reparo, como es el caso de Rusia y Ucrania, quienes se han atacado mutuamente desinformando en redes sociales y generando un sinnúmero de sentimientos contradictorios en las personas del mundo (Agencias Externas, 2024).

Amenazas: Los Estados deben ser más audaces y en eso trabajan constantemente, pues deben crear y evaluar estrategias ajustadas a posibles contextos que se puedan presentar. Esto con el fin de analizar diferentes perspectivas y escenarios que otros países pudiesen contemplar para dañar su estructura, respondiendo así de modo acertado y preciso a las amenazas que afrontan en el ciberespacio (Zambrano, 2022).

Efectos: Las ciberarmas obtienen aspectos negativos como: económicos, psíquicos, sociales, estatales y militares. La pérdida de la privacidad e información es un aspecto importante tanto para la sociedad como para el país, pues en ello radica un sinnúmero de historia y aprendizaje de la evolución del mismo (Niss, 2023).

Ciberseguridad

La industria de la ciberseguridad juega un papel fundamental en la defensa de infraestructuras críticas y la protección contra ciberataques. De acuerdo con Ramírez (2021), la ciberseguridad ha evolucionado como un componente fundamental de la seguridad nacional, integrando medidas preventivas, capacidades de respuesta y normativas que fortalecen la resiliencia de los Estados frente a ciberamenazas.

Dado lo anterior, es importante detallar dos aspectos importantes de la ciberseguridad, para el contexto militar y la defensa de cada país: la cooperación y la respuesta a incidentes.

Cooperación: La colaboración mutua entre los gobiernos del mundo es decisiva, para gestionar leyes y normatividad que regule esta práctica y en el que ideen acuerdos que favorezca a todos frente a la ciberseguridad, pues de esta manera se sabe los límites que cada uno debe cumplir en favor de la paz y seguridad mundial (Rivera y Hernández, 2023).

Respuesta a incidentes: Es importante que cada país diseñe, gestione y evalué protocolos de réplica a ciberataques para reducir el daño, clasificar la amenaza y restituir la funcionalidad de los sistemas. Pues esto permite evaluar constantemente los posibles escenarios de ataque y cómo es su respuesta, llevando a evaluar los recursos, la planeación, gestión y evaluación de las medidas sugeridas e implementadas (Mogollón, 2021).

Finalmente, la ciberseguridad requiere de una evaluación constante para los posibles escenarios de ataque en el que detalle los recursos, el apoyo, la regulación y la cooperación internacional.

Ciberseguridad y Defensa Nacional: Un Desafío Global

Una característica que se debe observar detenidamente de la ciberseguridad, es los no límites a diferencia de las coacciones tradicionales, mientras que estas perturbaciones cibernéticas pueden causarse en cualquier lugar del mundo e inquietar a varios países juntamente. Esto ha permitido el diseño e innovación de convenios internacionales y el progreso de normativas globales, cuya finalidad es afrontar peligros de forma unida.

Capacidades tecnológicas y tácticas de ciberdefensa de Estados Unidos y Rusia

Las capacidades tecnológicas y tácticas de ciberdefensa de dos potencias como Estados Unidos y Rusia, generan un sinnúmero de enseñanzas para otros países, pero también de intimidación, pues no solo se esfuerzan en experimentar diferentes escenarios posibles de ataque cibernético, sino que buscan ser lideres en la implementación de prácticas, políticas y tecnología que les permita encabezar el ranking para disuadir a los demás. Por esa, razón se va a detallar el actuar de estos dos países en el siguiente cuadro comparativo.

Tabla 1. Capacidades tecnológicas y tácticas de Estados Unidos y Rusia.

Dimensión	Estados unidos	Rusia
Capacidades tecnológicas		
Estructura institucional	USCYBERCOM NSA / DHS / FBI Coordinación interagencial Civil-militar (Fortune Business Insights, 2025).	Ministerio de Defensa GRU (inteligencia militar) FSB Control centralizado y opaco del entorno digital (CISA, 2022).
Cooperación Internacional	OTAN Five Eyes Tratados bilaterales Iniciativas multilaterales de ciberseguridad. (Fortune Business Insights, 2025).	Colaboración restringida (especialmente con China, Irán, Bielorrusia) Visión soberanista del ciberespacio (CISA, 2022).
Enfoque normativo	Estrategias nacionales (2018- 2023) Leyes de atribución y sanción Gobernanza multilateral (Niss, 2023).	Ambigüedad jurídica Ausencia de marcos transparentes Manipulación de la ley para control interno (CISA, 2022).
Rol del sector privado	Activo y cooperativo (Microsoft, Google, FireEye, etc.) Participación en defensa, detección e innovación (Niss, 2023).	Subordinado al Estado Empresas obligadas a cooperar con inteligencia Débil autonomía operativa (Niss, 2023).

Incidentes representativos	Stuxnet (2010) SolarWinds (2020, respuesta investigativa) Respuesta a Colonial Pipeline (2021). (Secureframe, 2024).	Not Petya (2017) Blackout Ucrania (2015-2016) Múltiples campañas de desinformación electoral (CISA, 2022).
Objetivos estratégicos en ciberespacio	Protección de democracia Disuasión de actores estatales y no estatales Superioridad cibernética ((Niss, 2023).	Expansión de influencia Erosión de democracias occidentales Debilitamiento institucional de adversarios (Niss, 2023).
	Tácticas	
Doctrina Estratégica	Defensa persistente Superioridad cibernética Enfoque completo de disuasión (Secureframe, 2024)	Guerra híbrida Dominación de datos Desestabilización política, económica, militar o social. Negación de forma fidedigna su alcance en una operación. (CISA, 2022).
Desarrollo Tecnológico	Criptografía Ciberresiliencia Ecosistema abierto I+D en IA Big data Cloud computing Colaboración público-privada (Silicon Valley) (Niss, 2023).	Ciberataques sofisticados, control interno Desarrollo limitado Fuerte dependencia estatal Inversión en tecnologías de control (SORM, RuNet) (CISA, 2022).
Tácticas ofensivas	Ciberoperaciones activas Neutralización de infraestructura enemiga Desarrollo de capacidades autónomas (Patino, 2021).	Ciberataques encubiertos Sabotaje de infraestructuras críticas Operaciones de influencia y propaganda (CISA, 2022).
Tácticas defensivas	Resiliencia sistémica Defensa de infraestructuras críticas Respuesta ante incidentes CISA y NIST (Fortune Business Insights, 2025).	Protección interna mediante filtrado y monitoreo Control del tráfico digital Control de las ideas o expresiones (Patino, 2021).

Fuente: elaboración propia en base a la consulta de CISA, 2022; Fortune Business Insights, 2025; Niss, 2023; Patino, 2021 y Secureframe, 2024.

La tabla anterior permite visualizar un gran actuar de Estados Unidos y Rusia en cuanto al manejo de su ciberdefensa y ciberseguridad, sin embargo, hay puntos estratégicos que cabe resaltar:

Para empezar el análisis de las capacidades tecnológicas, se procede por la dimensión de la estructura institucional en la que Estados Unidos detalla un enfoque organizado y sistemático, basado en el principio de la cooperación civil-militar cuyo marco normativo e institucional, se fortalece hacia una dirección de resiliencia estructural, que involucra tanto al sector público como al privado. Mientras que Rusia, no tiene una estructura consolidada, más que las acciones que ejecuta según la ofensiva que reciba, en la que irrespeta a las instituciones ejerciendo presión y manipulación de información y redes (Rodeheffer, 2025).

En cuanto a la cooperación internacional, Estados Unidos cuenta con varios aliados iniciando por la OTAN y otros más, por el contrario, Rusia tiene una colaboración restringida (especialmente con China, Irán, Bielorrusia). Así que por el lado del enfoque normativo: Estados Unidos dispone de varias normas como las estrategias nacionales (2018- 2023) y otras, buscando la actualización de procesos y la mejora de sus leyes; por el contrario, Rusia presenta ambigüedad jurídica, ausencia de marcos transparentes y manipulación de la ley para control interno (Pringle, 2025).

Con respecto al rol del sector privado, Estados Unidos, tiene el apoyo activo y cooperativo de grandes organizaciones como es Microsoft, Google, etc.; por el lado de Rusia, ejecuta una subordinación al Estado, ya que obliga a las empresas a cooperar con inteligencia y débil autonomía operativa. Demostrando así, que las alianzas son importantes y que, a pesar de buscar el liderazgo, la opinión y acciones en conjunto impulsan a una mejor evaluación y actuar.

Por el lado de los Incidentes representativos, Estados Unidos ha evidenciado varios, lo que lleva a precisar la experiencia que ha adquirido y la organización con la que cuenta,

lo contrario de Rusia que enfatiza en múltiples campañas de desinformación electoral, sin que esto tenga un mayor actuar, más que defenderse en el momento más no proyecta a un futuro su estrategia.

Y para terminar las capacidades tecnológicas están los Objetivos estratégicos en ciberespacio, que por el lado de Estados Unidos trabaja arduamente en la protección de la democracia, la disuasión de actores estatales y no estatales y superioridad cibernética. Lo contario de Rusia, la cual expande su influencia y debilita a las institucional de los contrincantes.

Seguidamente se analizará las dimensiones de las tácticas, en las cuales se inicia por la doctrina estratégica en ella Estados Unidos demuestra una defensa persistente, un liderazgo notable por la superioridad cibernética y enfoque completo de disuasión, permitiéndole llevar una gran delantera. Lo contrario de Rusia, la cual manipula información, desestabiliza la política, economía, militar y social de los contrincantes y actuar no ético, pues niega su actuar.

Por el lado del desarrollo tecnológico, Estados Unidos, trabaja y busca constantemente posibilidades de trabajo como la criptografía, I+D en IA, Big data, etc. Muy diferente de Rusia, quien ataca desde el control interno, no tiene un desarrollo amplio y solo ha invertido en tecnologías de control como SORM y RuNet (CISA, 2022).

Posteriormente las tácticas ofensivas, en las que Estados Unidos simula sinnúmero de ataques que le permita evaluar todo el proceso de respuesta y le genere nuevas formas de ataque, en tanto que Rusia ejecuta ciberataques escondidos, sabotea infraestructuras críticas y persuade a través de la propaganda e influencia.

Y las tácticas defensivas que, por el lado de Estados Unidos, analiza la protección a su infraestructura crítica y evalúa la posibilidad de atacar a otros en este sentido si fuera necesario y simula respuestas ante incidentes, al tiempo que Rusia usa protección interna mediante filtrado y monitoreo, controla el tráfico digital, ideas o expresiones, siendo obsoleta su forma de actuar y con pocas herramientas.

Finalmente, es posible deducir que Estados Unidos prima un enfoque estructurado, multilateral, técnicamente evolucionado y normativamente organizado, con lo cual accede a preservar un entorno ciber defensivo complejo pero eficiente. Su doctrina de "defensa ininterrumpida" busca no solo abogar sus redes, sino también operar dinámicamente para desalentar amenazas antes de que se materialicen (Antonio, 2025). Por el contrario, Rusia articula su ciberdefensa al interior de una lógica de poder informacional, en la cual el objetivo central no es exclusivamente defenderse, sino utilizar el ciberespacio como mecanismo estratégico de confrontación desnivelado, desestabilización y manipulación narrativa a escala global (Kristiansen, 2021).

Evaluación de Estrategias de prevención, detección y respuesta ante ciberataques de Estados Unidos y Rusia.

Estrategias de prevención

Las estrategias de prevención se componen de una serie de ejercicios, políticas, instrucciones y tecnologías encaminadas a anticipar, reducir o suprimir los riesgos derivados del uso de sistemas informáticos, redes digitales y dispositivos conectados. Estas estrategias buscan proteger la privacidad, integridad y disponibilidad de la información frente a

amenazas cibernéticas como malware, phishing, ransomware, accesos no autorizados, entre otros (Kristiansen, 2021).

A continuación, en la Tabla 2, se detallan los enfoques y acciones que ejecutan los países de Estados Unidos y Rusia en pro de la ciberdefensa de cada uno.

Tabla 2 Estrategias de Prevención de Estados Unidos y Rusia.

Estrategias	Estados Unidos	Rusia
Enfoque	Estrategia global orientada a la doctrina de "defensa en profundidad" (defense-in-depth) (OEA, 2023).	Estrategia preventiva a partir del seguimiento estatal en el ciberespacio, sistema SORM (Sistema Operativo de Medidas de Investigación) (Kristiansen, 2021).
	Alianza interagencial Alianzas internacionales Alianzas con el sector privado (OEA, 2023).	Impone a operadores de red a proveer acceso abierto a las agencias de seguridad para fines de monitoreo (Kristiansen, 2021).
Acciones	Ejecución de leyes de ciberseguridad obligatorias en sistemas críticos (Cybersecurity and Infrastructure Security Agency) (OEA, 2023).	Proyecto de "internet soberana" (RuNet), en la que aísla el tráfico nacional del internacional ante un peligro externo. Sin embargo, esta prevención es más reactiva que preventiva, basada en reprensión, contención tecnológica y vigilancia doméstica. (Kristiansen, 2021).
	Implementación de normas técnicas y uniformidad de buenas prácticas en sectores público y privado, como el NIST Cybersecurity Framework (OEA, 2023).	
	Inversión en ciber educación, entrenamiento nacional e instrucciones multinacionales como "Cyber Storm" (OEA, 2023).	

Fuente: elaboración propia en base a Kristiansen, 2021 y OEA, 2023.

Para concretar, Estados Unidos extiende un modelo abierto, normativo y cooperativo de gestión del riesgo cibernético, encaminado a la prevención proactiva, la detección temprana automatizada de los posibles riesgos internacionales, evaluación de las herramientas usadas y la respuesta rápida y proporcional ante cualquier contienda mundial.

En cambio, Rusia acoge una estrategia calculada en la inspección del gobierno en el ciberespacio y la represalia desigual, favoreciendo la manipulación informativa y el ocultamiento operacional.

Finalmente, al anticiparse a posibles amenazas mundiales como lo hace Estados Unidos, lleva a contemplar una magnitud desproporcional de riesgos y posibles acciones procedentes de otras partes del mundo, pues al contrarrestarlas precisa las herramientas necesarias para ejecutar los planes que constantemente evalúan, lo contrario de Rusia el cual actúa de manera inmediata más no anticipatoria que le permita inspeccionar sin número de acciones y herramientas necesarias para proteger su territorio.

Estrategias de detección

Las estrategias de detección contemplan un conjunto de mecanismos, metodologías e instrumentos orientadas a precisar de manera anticipada actividades maliciosas, accesos no autorizados o comportamientos inusuales al interior de una red o sistema informático. Estas buscan examinar cuándo y cómo ocurrió o puede ocurrir una amenaza, para poder frenarla y mitigar sus efectos.

En la tabla 3, se detallan los enfoques y acciones que ejecutan los países de Estados Unidos y Rusia en pro de la ciberdefensa de cada uno.

Tabla 3 Estrategias de Detección de Estados Unidos y Rusia.

Estados Unidos	Rusia
Enfoque: Automatizado Distribuido Colaborativo Usa: Inteligencia artificial Algoritmos de aprendizaje automático Redes de sensores avanzados (National Institute of Standards and Technology, 2024).	Centraliza su capacidad de detección en la vigilancia interna extenuante y en las operaciones de contrainteligencia técnica realizadas por el FSB y el GRU (CISA, 2022).

Herramientas	
Einstein 3, sistema de detección de intrusiones de nivel federal manejado por el DHS, que rastrea tráfico de red en persecución de amenazas conocidas (Hassan, Haroon, Khalid y Ghayoor, 2024).	Existen mecanismos de supervisión digital sobre redes sociales, servicios de mensajería y proveedores de telecomunicaciones. Sin embargo, la detección no se basa en estándares abiertos ni en transparencia, sino en vigilancia masiva y control de datos centralizados (Hassan, Haroon, Khalid y Ghayoor, 2024).
National Cybersecurity Protection System (NCPS), que vigila amenazas mediante big data y análisis de comportamiento ((Hassan, Haroon, Khalid y Ghayoor, 2024).	
Colaboración con empresas privadas (Microsoft, CrowdStrike, etc.) para supervisión compartida de amenazas globales (Hassan, Haroon, Khalid y Ghayoor, 2024).	Esta estrategia detecta amenazas percibidas desde el exterior (como disidencia digital), pero puede carecer de adaptabilidad frente a amenazas técnicas emergentes o actores no estatales sofisticados (CISA, 2022).

Fuente: elaboración propia en base a los autores CISA, 2022; National Institute of Standards and Technology, 2024 y Hassan, Haroon, Khalid y Ghayoor, 2024.

Con base en la anterior tabla se puede concluir que, la importancia de las estrategias de detección para los países de Estados Unidos y Rusia en la ciberseguridad nacional se puede observar desde 3 perspectivas: 1) Protección de infraestructuras críticas, sectores como energía, salud, financiero, defensa y transporte dependen de sistemas informáticos. Un error puede tener repercusiones devastadoras para la seguridad nacional y el bienestar del pueblo. 2) Defensa frente a ciber conflictos y ciberterrorismo, las estrategias de prevención y detección consienten anticipar, frenar y responder ante posibles agresiones cibernéticas internacionales, que quieren perturbar al Estado o influir en sus procesos políticos. 3) Fortalecimiento de la confianza digital, la puesta en práctica de esas estrategias afianza la confianza de los ciudadanos y empresas en el entorno digital, lo que es imprescindible para la economía digital, el comercio electrónico, la educación virtual y los servicios gubernamentales en línea; y 4) Resiliencia institucional y soberanía tecnológica, un país que invierte en pericias de detección y prevención, refuerza su soberanía tecnológica y baja su

dependencia de proveedores externos, para así incrementar su capacidad de respuesta autónoma frente a incidentes.

Estrategias de respuesta

Las estrategias de respuesta establecen actividades, políticas, protocolos y potencial técnico para contener, mitigar, investigar y recuperar el impacto de incidentes cibernéticos una vez que este ha sucedido. Estas estrategias son contragolpe natural, aun así, son esenciales para la estructura de seguridad integral junto a las estrategias preventivas y de detección.

En la tabla 4, se dan a conocer las respuestas que ejecutan los países de Estados Unidos y Rusia en pro de la ciberseguridad de cada.

Tabla 4 Estrategias de respuesta de Estados Unidos y Rusia.

	Estados Unidos	**Rusia**
Niveles	*Táctico*: participación rápida ante atentados a través de equipos especializados Cybersecurity Incident Response Teams - CSIRTs) (Cybercom, 2023).	Se enfoca en acciones disimuladas, retaliación asimétrica y negación convincente. En vez de informar públicamente los ataques sufridos, opta por enfrentar de manera silenciosa o a través de operaciones paralelas, como campañas de desinformación, ciberespionaje o retaliaciones en terceros países. Además, no separan tiempos de paz y conflicto, lo que le consiente operar en la "zona gris" del derecho internacional (D´Cunha, Rodenhauser y Ferraro, 2025). Su marco normativo no incorpora estructuras institucionalizadas de coordinación civil ante ciber crisis, y la respuesta suele estar centralizada en el aparato de inteligencia militar. (D´Cunha, Rodenhauser y Ferraro, 2025).
	Operacional: coordinación a través de USCYBERCOM para llevar a cabo contraataque ofensivo, entre ellos el despliegue de malware neutralizador, como sucedió en las operaciones en contra del Estado Islámico (Cybercom, 2023).	
	Estratégico y legal: imposición de sanciones internacionales, imputación pública de ataques (naming & shaming), y aplicación del principio de respuesta proporcional en el ciberespacio (Cybercom, 2023).	

Fuente: elaboración propia en base a los autores D´Cunha, Rodenhauser y Ferraro, 2025 y Cybercom, 2023.

Es importante analizar la organización que Estados Unidos ejecuta en favor de la ciberdefensa para su seguridad nacional, pues se acompaña de varios programas en los que actúa desde diferentes ángulos como lo es, la anticipación: en la que busca simular invasiones externas de tal forma que le permitan evaluar su actuar y herramientas para arremeter dicha amenaza, la actualidad, en esta evalúa diferentes escenarios de acuerdo a las capacidades de sus oponentes en las que revisa y ajusta si es necesario sus planes; y futuro, le permite basarse en sus experiencias y actuar de los demás para innovar nuevas acciones, herramientas y políticas.

En cambio, Rusia, es un país que actúa en reacción a la amenaza que enfrente en la actualidad, no cuenta con una preparación previa ni posterior que lo lleve a adquirir experiencia y evaluaciones previas que le permitan prepararse y evaluar a sus oponentes externos. Improvisar en la seguridad nacional, llevara a una pérdida de recursos, a una diminuta capacitación y a defender el territorio con lo que puede, más no con lo organizado anticipadamente.

Incidentes cibernéticos relevantes de Estados Unidos y Rusia

Los incidentes cibernéticos son actividades que amenazan la confidencialidad, integridad o acceso a la información, los sistemas informáticos, las redes o los servicios digitales. Estos incidentes pueden ser originado por actos maliciosos, equivocaciones humanas, falencias técnicas o fragilidades gestionadas de manera intencional o accidental. Al respecto, el manejo de incidentes cibernéticos implica un conjunto de acciones planeadas que consienten identificar, contener, eliminar y recobrar sistemas ante un evento adverso. Desde un enfoque estratégico, los países deben disponer de un Plan de Respuesta a Incidentes

(PRI), personal capacitado y tecnologías actualizadas, que concedan actuar de forma eficiente y reducir los riesgos externos (OEA, 2023).

Ejecutados por Estados Unidos

En primer lugar, se detallará los incidentes cibernéticos de Estados Unidos hacia Israel, Irán, Estado Islámico y Rusia, en los que se desglosa el incidente y la estrategia defensiva.

Tabla 5 Incidentes Cibernéticos de Estados Unidos hacia otros países.

Ejecutados por Estados Unidos
2010 – Stuxnet / Programa nuclear iraní Incidente: Ciberataque a través de un malware destinado a sistemas SCADA, para demorar la evolución nuclear iraní sin aplicar la fuerza militar directa. Estrategia Defensiva: – Explotó cuatro vulnerabilidades "zero-day" en Windows. – Se infiltró mediante USB y redes internas desconectadas (air-gapped). – Manipuló controladores industriales (Siemens S7 PLCs), afectando velocidades de rotación mientras enviaba señales normales a los sistemas de monitoreo (CISA, 2024).
2007/2010 - Operación Olympic Games / Programa de enriquecimiento de uranio de Irán Incidente: Sabotear discretamente a la planta de Natanz, sin recurrir a bombardeos o intervenciones militares. Conexión: Incluye Stuxnet (gusano informático que afecta a equipos con Windows), parte de una campaña secreta extensa. Herramienta clave: Desarrollo del malware Stuxnet, considerado la primera arma cibernética físico-digital de la historia (Ruiz, 2025).
2007/2013 - Operación PRISM y XKeyscore / Programa de uranio de Irán Incidente: Vigilancia masiva global de comunicaciones Objetivo: Sabotear discretamente el programa de enriquecimiento de uranio de Irán en la planta de Natanz, sin acudir a bombardeos o intervenciones militares. Estrategia Defensiva: – Irán víctima del ataque (Creación de comandos cibernéticos, segmentación OT/IT, contraataques digitales). – Organismos internacionales. Regulación de seguridad cibernética nuclear (IAEA, NIST, ENISA). – Fortalecimiento del escudo SCADA de EEUU, políticas de ciberresiliencia nacional (Antonio, 2025).

2016/2018 - Operaciones ofensivas de la NSA y el Cyber Command (USCYBERCOM) a) Intervenciones contra grupos vinculados al Estado Islámico (2016–2017): USCYBERCOM ejecutó la Operation Glowing Symphony, dirigida a deteriorar redes de comunicación y propaganda del ISIS. b) Operaciones contra infraestructura crítica rusa (desde 2018): Instauración de malware y puertas traseras en redes del sistema eléctrico ruso. El objetivo fue disuadir y capacidad de represalia en caso de conflicto híbrido (Expósito, 2021).

Fuente: elaboración propia en base a los autores CISA, 2024; Antonio, 2025; Expósito, 2021 y Ruiz, 2025.

De acuerdo con la información consignada en la T*abla 5 Incidentes Cibernéticos de Estados Unidos hacia otros países, s*e detalla la doctrina ofensiva ejecutada como estándar de seguridad nacional. En primera instancia los incidentes cibernéticos Stuxnet y Olympic Games de EE.UU. hacia Israel, formalizo la implementación de operaciones cibernéticas ofensivas como herramienta de su política exterior y defensa, consolidando esas acciones dentro de su doctrina de disuasión digital activa. Esta perspectiva ha sido concertada a través de documentos como la National Cyber Strategy (2018) y la estrategia "Defend Forward" de USCYBERCOM.

Desde un segundo panorama, la ambigüedad legal de las PRISM y XKeyscore tuvo controversias importantes, en las que se señaló la violación al derecho de la privacidad, en especial de ciudadanos extranjeros y líderes de Estados aliados. En cuanto a Stuxnet, al ser un ataque sin precedentes a una infraestructura civil de un país no agresivo, abrió discusiones en cuanto a la proporcionalidad, atribución y derecho internacional humanitario.

Seguidamente, el crecimiento de amenazas proporcionadas en el actuar ofensivo estadounidense, incentivo la formación de capacidades similares por parte de otras potencias: Rusia con grupos como APT28 y Sandworm; China con APT10 y operaciones como Clodhopper e Irán con APT33, responsable de ataques a Saudi Aramco.

Finalmente, las intervenciones para países intermedios como Colombia o naciones de América Latina, el precedente de estas operaciones demuestra: la necesidad de fortalecer la ciberresiliencia nacional, incluyendo el sector energético, militar y civil; el riesgo de convertirse en escena indirectas o teatros de prueba de conflictos geopolíticos cibernéticos y la celeridad de fijar marcos normativos internos e internacionales para regular la ciberguerra, la atribución y la defensa activa.

Realizados contra Estados Unidos

Se precisará los incidentes cibernéticos más importantes que Rusia, China y Corea del Norte han emprendido contra Estados Unidos, en los que se desglosa el incidente y la estrategia defensiva.

Tabla 6 Incidentes Cibernéticos contra Estados Unidos.

Contra Estados Unidos
2021 - Colonial Pipeline Attack / vínculos rusos indirectos Incidente: Ransomware dirigido a infraestructura crítica. Estancamiento temporal del oleoducto más importante del sureste de EE. UU. Afectó el suministro de gasolina, diésel y combustible para aviación. Estrategia defensiva: – Las redes OT/ICS deben aislarse lógicamente de redes IT para evitar propagación de malware. – Colaboración entre el FBI y CISA fueron decisivas y rápida para recuperación de activos. – Se reafirmo el inicio de responsabilidad soberana sobre actores cibernéticos en el propio territorio. – Se reforzo el marco obligatorio de seguridad para el sector energético y de transporte. (CISA, 2024).
2020 – SolarWinds / Rusia (grupo APT29) o "Cozy Bear", vinculado al SVR. Incidente: Perjudicó actualizaciones del software Orion de SolarWinds, usado por más de 18,000 entidades en todo el mundo. Estrategia defensiva: – Contención técnica con una orden de emergencia a todas las agencias federales. – Coordinación interinstitucional (creación Cyber Unified Coordination Group). – Sanciones económicas, diplomáticas y reforma de ciberseguridad federal. – Expulsión de diplomáticos rusos. (Antonio, 2025).

2021 - Microsoft Exchange Server Exploits / China (group Hafnium) Incidente: Más de 250.000 servidores afectados en todo el mundo. Se ingreso a buzones de correo, redes internas y credenciales empresariales. El ataque combinó ciberespionaje con sabotaje automatizado. Estrategia defensiva: – Descubrimiento de múltiples vulnerabilidades día cero. – Elaboraron guías técnicas sobre mitigación temporal. – Se activaron protocolos de ciberseguridad defensiva compartida entre el gobierno y el sector privado (Joint Cyber Defense Collaborative). – Intervención legal (orden judicial para que el FBI interviniera) y neutralización remota (Se eliminaron *web shells* maliciosos insertados por Hafnium). – Atribución y respuesta diplomática (Estados Unidos, Unión Europea, Reino Unido, Canadá, Australia y Japón imputaron oficialmente el ataque a grupos afiliados al gobierno de China). – Se afianzo la necesidad de limitar la dependencia de infraestructura on-premise expuesta (Expósito, 2021).
2017 - Equifax Breach / China (Ejército Popular de Liberación, APT41) Incidente: Perjudico la información de 147 millones de ciudadanos estadounidenses, a los cuales se les extrajeron nombres, números de seguridad social, fechas de nacimiento, domicilios y datos financieros. Estrategia defensiva: – Manejo de herramientas de monitoreo y seguimiento para imputar el ataque a actores estatales. – Enjuiciamiento simbólico a militares chinos ante tribunales estadounidenses. – Deber legal de reestructurar protocolos y arquitectura de seguridad. – Fortalecimiento de la cultura de cumplimiento y normativa sobre empresas que administran datos críticos. (Secureframe, 2024).
2015 - Office of Personnel Management Breach / China (group APT10) Incidente: Robo de información clasificada de más de 22 millones de empleados federales. Se perjudico datos biométricos, historiales laborales, de seguridad y formularios SF-86. Estrategia defensiva: – Uunificación de la gestión de ciberseguridad federal en DHS. – Aadopción de autenticación multifactor, cifrado y segmentación de red. – Conformación de nuevos órganos como el NBIB y fortalecimiento del CDM. – Disuasión basada en acuerdos y tensión multilateral más que en sanciones. (Ruiz, 2025).
2014 - Sony Pictures Hack / Corea del Norte (grupo Lazarus). Incidente: Borrado de archivos, filtración de correos internos y publicación de películas inéditas. Motivado por la película "The Interview, que ridiculizaba al régimen norcoreano". Sony detuvo su estreno temporalmente. Estrategia defensiva: – Refuerzo del rol del FBI y NSA en investigación y atribución cibernética. – Sanciones e imputación pública como instrumento de disuasión estatal. – Sony transformó su postura de ciberseguridad de reactiva a preventiva. (CISA, 2024).

Fuente: elaboración propia en base a los autores CISA, 2024; Antonio, 2025; Expósito, 2021, Ruiz, 2025 y Secureframe, 2024.

A partir de los datos presentados en la *Tabla 7 Incidentes Cibernéticos contra Estados Unidos*. Los incidentes cibernéticos analizados: Colonial Pipeline, SolarWinds, Microsoft Exchange Exploits, Equifax, OPM Breach y Sony Pictures Hack, exponen una continua atención en la estructura de ciberseguridad estadounidense: el desajuste creciente entre el poder ofensivo del país y su fragilidad estructural en la defensa digital. A pesar de contar con una de las infraestructuras tecnológicas más avanzadas del mundo, Estados Unidos ha demostrado debilidades en aspectos esenciales como:

- El manejo oportuno de fragilidades conocidas, como en el caso de Equifax y Microsoft Exchange.
- La protección de infraestructuras críticas, como demostró el ataque a Colonial Pipeline, que generó déficit energético temporal en la costa este.
- La seguridad de los sistemas federales y la privacidad de los datos personales, como se reflejó en OPM Breach, que amenazo la seguridad nacional.
- La capacidad de resiliencia institucional frente a ataques con componentes simbólicos, ideológicos o geopolíticos, como el hackeo a Sony Pictures, que excedió lo financiero y representó una forma de censura estatal transnacional.

En un enfoque estratégico, estos incidentes evidencian la transformación del ciberespacio desde un dominio técnico irrelevante hacia un escenario central de conflicto y competencia interestatal.

Finalmente, estos ataques no solo establecen episodios de inseguridad digital, sino que equivalen a manifestaciones contemporáneas de poder desigual y conflicto sistémico en

la era informacional. Como tal, necesitan un enfoque integral, interdisciplinario y transversal a todas las esferas de la seguridad nacional y global.

Ejecutados por Rusia

A continuación, se expone los incidentes cibernéticos más importantes que Rusia emprendió hacia países como Estonia, Georgia, Ucrania, Alemania, Estados Unidos y Ucrania, en los que se desglosa el incidente, a quien iba dirigido el ataque, el objetivo y la estrategia defensiva.

Tabla 8 Incidentes Cibernéticos de Rusia hacia otros países.

Ejecutados por Rusia
2007 - Ciberataques a Estonia Incidente: Ataques DDoS a infraestructura pública y privada tras conflicto político con Rusia. Dirigido a: Estonia. Objetivo: Saturación de sitios web gubernamentales, bancarios y medios. Primera ciberguerra registrada. Estrategia Defensiva: – Fortalecimiento del *CERT-EE* y creación del Centro de Ciberdefensa Cooperativa de la OTAN (CCDCOE) en Tallin en 2008. – Ejecución de políticas de ciberresiliencia en infraestructuras críticas. – Digitalización blindada mediante segmentación de redes y redundancias nacionales. (Kristiansen, 2021).
2008 - Guerra cibernética en Georgia Incidente: Coordinación entre ciberataques y conflicto militar en Osetia del Sur. Dirigido: Georgia Estrategia Defensiva: – Asistencia técnica de Estonia y EE. UU. para restablecer conectividad. – Reorganización de infraestructura digital crítica con apoyo OTAN. – Adopción de estrategias de respaldo físico (copias impresas y satelitales) para comunicaciones. (CISA, 2022).

2014 - Operaciones contra Ucrania
Incidente: Serie de ciberataques masivos, incluyendo apagones eléctricos, ransomware (*NotPetya*), malware destructivo (*Industroyer*, *HermeticWiper*).
Dirigido: Ucrania
Estrategia Defensiva:
- Creación de Cibercomando Militar Ucraniano y cooperación directa con EE. UU., Reino Unido, OTAN.
- Desarrollo de capacidades internas de detección (CERT-UA) y alianzas con firmas privadas como Mandiant y Microsoft.
- Estrategia defensiva basada en ciberseguridad ofensiva, resiliencia digital descentralizada.
- Implementación de "copias espejo" gubernamentales en servidores en el extranjero.

(Kristiansen, 2021).

2015 - Hackeo al Bundestag alemán
Incidente: Robo de correos electrónicos y documentos sensibles del parlamento alemán.
Dirigido: Alemania
Estrategia Defensiva:
- Creación de la Oficina Federal para la Seguridad de la Información (BSI).
- Fortalecimiento del Comando de Ciberdefensa de la Bundeswehr (2017).
- Sanciones de la UE y demanda penal contra hackers vinculados al GRU.

(Expósito, 2021).

2016 - Interferencia en las elecciones de EE. UU.
Incidente: Hackeo al DNC y campañas masivas de desinformación digital.
Dirigido: Estados Unidos
Estrategia Defensiva:
- Activación del Departamento de Seguridad Nacional (DHS) y la NSA para protección electoral.
- Creación de la Cybersecurity and Infrastructure Security Agency (CISA).
- Sanciones a Rusia, cierre de consulados, expulsión de diplomáticos.
- Conexión desinformación.

(CISA, 2022).

2017 - Ataques globales de malware: NotPetya y otros
Incidente: Malware destructivo disfrazado de ransomware, con origen en Ucrania, pero efectos globales.
Dirigido: Empresas multinacionales (Maersk, FedEx, Merck), gobiernos europeos, bancos, Ucrania.
Estrategia Defensiva:
- EE. UU., Reino Unido y la OTAN emitieron atribución oficial conjunta al GRU ruso (Sandworm).
- Empresas afectadas crearon estrategias de *Zero trust*, segmentación de redes y respaldo offline.
- Naciones víctimas mejoraron estándares de seguridad SCADA y emprendieron detección de anomalías basada en inteligencia artificial.
- Inicio del desarrollo de normas internacionales sobre ciberataques destructivos (en G7 y ONU).

(Ruiz, 2025).

Fuente: elaboración propia en base a los autores CISA, 2022; Kristiansen, 2021; Expósito, 2021 y Ruiz, 2025.

Los incidentes cibernéticos atribuidos a Rusia entre 2007 y 2024 prueban una evolución consecuente y estratégica de su doctrina de proyección de poder en el ciberespacio, encuadrada en una lógica de guerra híbrida, desinformación estructural y sabotaje digital. A diferencia de ataques cibernéticos con fines únicamente criminales o financieros, las operaciones rusas se han acentuado por perseguir objetivos políticos, militares y geoestratégicos, dirigidos a perturbar gobiernos, violar infraestructuras críticas, debilitar la cohesión institucional y generar incertidumbre informativa.

Entre los casos analizados como los ataques a Estonia (2007), Georgia (2008), Ucrania (2014), el Bundestag alemán (2015), las elecciones estadounidenses (2016) y la propagación del malware NotPetya (2017), se observa un progreso tanto, en la complejidad técnica como en la coordinación táctica de los ataques. A lo largo de este período, actores vinculados al Estado ruso, como APT28, APT29 y Sandworm, han realizado un amplio inventario de herramientas: malware modular, Exploits de día cero, ataques de denegación de servicio (DDoS), spear phishing, wipers, y campañas de manipulación psicológica digital.

En respuesta, los Estados afectados han reforzado sus capacidades defensivas a través de la incorporación de comandos cibernéticos, el desarrollo de agencias de ciberseguridad técnica (CERT, CISA, BSI), y la implementación de normatividad nacional e internacional, dirigidos a la resiliencia, la adjudicación y la disuasión activa. Asimismo, el aumento de cooperación entre países europeos, Estados Unidos y estructuras como la OTAN ha unificado una estructura de defensa colectiva digital frente a amenazas persistentes avanzadas (APT).

No obstante, la naturaleza transfronteriza del ciberespacio, unido a las dificultades técnicas y jurídicas de la atribución, formula retos considerables para el derecho internacional

y la gobernanza global. Los casos documentados evidencian que laos ataques cibernéticos rusas no solo tienen un impacto tecnológico, sino también consecuencias geopolíticas duraderas, al debilitar la confianza en procesos electorales, deteriorar la estabilidad económica y debilitar la soberanía informativa de los Estados.

Como cierre, se vuelve imprescindible que los países afectados refuercen su cultura de ciberresiliencia, impulsen estándares comunes de ciberseguridad, y avancen hacia un consenso internacional sobre la reglamentación de operaciones cibernéticas ofensivas en tiempos de paz. Sin tales medidas, el ciberespacio seguirá siendo un terreno productivo para la confrontación estratégica secreta, con impactos cada vez más tangibles sobre la seguridad nacional e internacional.

Realizados contra Rusia

Del mismo modo, se expone los incidentes cibernéticos más importantes que los países de Europa Occidental, América del Norte, Israel, Ucrania y Estados Unidos, han ejecutado contra Rusia y en los que se desglosa el incidente y la estrategia defensiva.

Tabla 9 Incidentes Cibernéticos contra Rusia.

Contra Rusia
2014 - Operación "Uroburos" / Agencias de inteligencia occidentales Incidente: Robo de información clasificada, vigilancia prolongada y compromiso de comunicaciones diplomáticas. Estrategia Defensiva: – Investigación técnica dirigida por Kaspersky Lab que llevó a la identificación del malware. – Aumento de las auditorías internas en redes estatales y migración de software occidental a plataformas nacionales (Linux Kaspersky OS). – Fortalecimiento del sistema GosSOPKA (Sistema Estatal Unificado de Detección, Prevención y Eliminación de Ataques Informáticos). (Kristiansen, 2021).

2022 - Ataque al satélite KA-SAT / Participación occidental y/ucraniana Incidente: Desconexión de terminales militares, interrupciones en comandos operacionales en fase inicial del conflicto. Estrategia Defensiva: – Redireccionamiento de sistemas de comando a redes militares terrestres (GLONASS y redes privadas). – Reforzamiento de medidas de seguridad en satélites militares (Cosmos series) y despliegue de ciber unidades espaciales. – Impulso a evolución de estructura de telecomunicaciones satelitales nacionales sin dependencia de operadores occidentales. (Expósito, 2021).
2023 - Operación Snake Malware Disruption / FBI, NSA, y aliados del grupo Five Eyes Incidente: Eliminación global del malware "Snake", instrumento usado por el FSB para espionaje internacional. Estrategia Defensiva: – Reestructuración de redes afectadas, regeneración de backdoors y diversificación de herramientas internas de ciberinteligencia. – Evolución de nuevas plataformas de espionaje digital (como Monokle y Cosmic Duke). – Refuerzo del sistema SORM (Sistema de Medición Operativa de Inteligencia) para vigilancia interna. – Aumento de turbiedad estatal sobre las capacidades cibernéticas y blindaje de documentación técnica crítica. (Ruiz, 2025).

Fuente: elaboración propia en base a los autores Kristiansen, 2021; Expósito, 2021 y Ruiz, 2025.

El análisis de la T*abla 8 Incidentes Cibernéticos contra Rusia,* revela que los ciberataques dirigidos contra la Federación Rusa desde el 2014 y con mayor intensidad desde 2022, divulgan un cambio de diseño en la conflictividad entre estados, donde el ciberespacio se afianza como un dominio estratégico para la confrontación geopolítica. La ejecución de operaciones ofensivas dirigidas por actores estatales, grupos activistas (como Anonymous) o coaliciones cívico-militares (como la IT Army of Ukraine), han mostrado que incluso potencias cibernéticas avanzadas como Rusia son frágiles a la exposición de sus redes gubernamentales, infraestructuras críticas, sistemas de telecomunicaciones y bases de datos sensibles.

Si bien Rusia ha respondido con el fortalecimiento del Runet, la expansión del sistema GosSOPKA, y el uso extensivo de mecanismos de censura interna, tales acciones priman el confinamiento por lo alto de la interoperabilidad, lo que amenaza su capacidad de adaptación ante ataques sofisticados y persistentes.

Desde la perspectiva de la seguridad nacional, estos eventos tienen tres impactos:

- Fragilidad estructural de activos críticos: La suspensión de servicios financieros, de transporte y de comando militar perjudica la continuidad operativa del Estado, alterando su proyección de poder y su estabilidad interna.
- Deterioro reputacional y pérdida de disuasión digital: La exposición pública de datos gubernamentales y el acceso externo a sistemas altamente delicados (como el correo electrónico presidencial o los registros militares) debilitan la percepción de invulnerabilidad que Rusia ha tratado de proyectar en el ciberespacio.
- Restricción en la doctrina de soberanía digital: Si bien la Federación ha impulsado un modelo soberano (Runet, software nacional, censura digital), los incidentes prueban que la autosuficiencia tecnológica no es suficiente frente a ciberamenazas internacionales mancomunadas, lo que plantea la necesidad de una gobernanza digital más resistente y colaborativa, incluso dentro de marcos geopolíticos adversos.

En suma, la experiencia rusa plasma que la ciberdefensa nacional no puede limitarse a una lógica estrictamente reactiva, autoritaria o militarizada. La protección integral del ciberespacio como activo de seguridad nacional necesita una estrategia multidimensional que

articule vigilancia técnica, resiliencia organizacional, educación digital de la ciudadanía y diplomacia cibernética preventiva. Al no existir tales medidas., el ciberespacio seguirá siendo un frente de fragilidad estratégica, aun para las potencias tecnológicas con mayores capacidades ofensivas.

Ciberseguridad nacional en perspectiva: contrastes entre EE. UU., Rusia y Colombia.

En el actual panorama de conflicto híbrido y transformación digital veloz, la ciberseguridad se ha consolidado como un componente estratégico de la seguridad nacional y el pronóstico geopolítico de las grandes potencias. En relación con ello, el análisis de los anteriores incidentes cibernéticos realizados por Estados Unidos y Rusia, demuestran la dimensión y complejidad de sus capacidades ofensivas y las lógicas geoestratégicas que sustenta a la ciberguerra moderna. Estos eventos de implicaciones globales (como Stuxnet, NotPetya, o las invasiones en infraestructuras críticas estadounidenses), instauran expresiones del poder cibernético gubernamental y permiten comprender los niveles de preparación, resistencia y doctrina de respuesta de cada país.

En esa línea, el análisis comparativo entre Colombia, Estados Unidos y Rusia ofrece un punto de vista analítico integral, sobre el grado de madurez de cada nación respecto a la ciberdefensa y ciberinteligencia. Mientras que Estados Unidos y Rusia han evidenciado capacidades operativas tanto defensivas como ofensivas a través de operaciones de magnitud internacional.

Dado lo anterior, Colombia enfrenta el reto de sentar un esquema cibernético robusto y autónomo, aprendiendo de los modelos, enseñanza y amenazas concretadas en dichos incidentes, buscando así proponer en base al modo operandi de EEUU y Rusia, el hallazgo de falencias que puedan servir como oportunidades de mejora al implementar una estrategia. De igual manera conocer herramientas y formas de preparación para cualquier ataque cibernético; demostrando dominio de la situación ante sus posibles contrincantes y experticia en diferentes prácticas en las que identifique todas las herramientas para un hecho real que se pueda presentar.

Tabla 10 Fortalezas de Colombia VS Estados Unidos y Rusia.

Dimensiones	Estados Unidos	Rusia	Colombia
Puntaje GCI (índice de competitividad global)	100/100 (1.º lugar mundial) (ITU, 2024).	98.06/100 (5.º lugar mundial) (ITU, 2024)	88.31/100 (63.º global, 3.º en América Latina) (ITU, 2024).
Enfoque estratégico	Múltiple: Defensa Resiliencia Protección de infraestructura crítica Respuesta Recuperación (OEA, 2023).	Geopolítico y ofensivo: Ciberespionaje Desinformación Desestimulo (Niss, 2023).	Defensivo y legal: Fortalecimiento institucional Marco legal (Díaz y Cremades, 2024).
Capacidad ofensiva	Confirmada y compleja (Stuxnet) operaciones de ciberespionaje evolucionado (ITU, 2024).	Muy alta e intensa (NotPetya, Fancy Bear, Cozy Bear)	Limitada o discreta; no se reportan operaciones ofensivas a nivel estatal (Díaz y Cremades, 2024).
Capacidad defensiva	Altamente desarrollada: Sistemas de alerta temprana SOCs (Centro de Operaciones de Seguridad) (ITU, 2024). CERTs (Equipo de Respuesta a emergencias Informáticas) Centros de mando (CISA, NSA, NIST) (ITU, 2024).	Focalizado en el control nacional y vigilancia; menor transparencia operativa (ITU, 2024).	En crecimiento; presencia del Centro Cibernético Policial y equipos (Computer Security Incident Response Team) en entidades públicas (Zambrano, 2022).
Marco normativo y legal	Super desarrollado: Ley de Ciberseguridad Nacional, Executive Orders, FISMA (Patino, 2021).	Centralizado, regido por el Kremlin; escasa independencia judicial (Niss, 2023).	En mejora: CONPES lineamientos en infraestructuras críticas (Mogollón, 2021).

Gobernanza institucional	Modelo federal con liderazgo técnico (CISA, USCYBERCOM, FBI, NIST, NSA) (Niss, 2023).	Modelo centralizado, militarizado (FSB, GRU, Roskomnadzor) (Patino, 2021).	Modelo multisectorial; presencia de Comisión Intersectorial de Seguridad Digital (Díaz y Cremades, 2024).
Ciberinteligencia y vigilancia	Desarrollo de capacidades de ciberinteligencia estratégica con respeto parcial de derechos civiles (Patino, 2021).	Sistema altamente intrusivo; uso extendido de vigilancia interna y desinformación (Niss, 2023).	Funciones limitadas; capacidades más centradas en la persecución de delitos informáticos (Zambrano, 2022).
Cooperación internacional	Alta: liderazgo en foros como el FIRST, OTAN, Five Eyes, OEA, G7, etc. (Patino, 2021).	Baja cooperación con Occidente; cooperación limitada con China, Irán, etc. (Patino, 2021).	Cooperación regional: OEA, BID, CSIRT Américas; participación en eventos OCDE y ONU (Mogollón, 2021).
Ecosistema académico y de I+D	Alta inversión en investigación aplicada y básica; colaboración con universidades y sector privado (Niss, 2023).	Fuerte desarrollo académico en criptografía, pero bajo acceso público (Patino, 2021).	Participación creciente, aunque dividido; programas en universidades como UNAL, U. Andes, U. Javeriana (Díaz y Cremades, 2024).
Formación y talento humano	Alta oferta de programas formativos y certificaciones (CyberCorps, NICE Framework, etc.) (ITU, 2024).	Formación centralizada para órganos estatales; menor democracia de la información (ITU, 2024).	Brechas importantes; insuficiencia de profesionales certificados y programas de alta especialización (Mogollón, 2021).
Protección de infraestructuras críticas	Presencia de sectores prioritarios identificados (electricidad, finanzas, salud); estrategia de gestión de riesgo (ITU, 2024).	Intervención estatal; uso de software nacional y segmentación de red (Niss, 2023).	Diagnóstico inicial; identificación de sectores críticos en fase inicial de implementación (Díaz y Cremades, 2024).
Madurez técnica-operacional (CSIRT, SOCs)	Altamente maduro; ecosistema variado con CSIRTs federales, sectoriales y privados (Niss, 2023).	Menor transparencia, al parecer existencia de CSIRTs militares (ITU, 2024).	Presencia de CSIRTs en policía y entidades estatales; (Mogollón, 2021).

Fuente: elaboración propia en base a los autores Díaz y Cremades, 2024; Mogollón, 2021; Patino, 2021; Niss, 2023; Zambrano, 2022; ITU, 2024 y OEA, 2023.

La tabla 6 permite apreciar las grandes potencias mundiales que son Estados Unidos y Rusia en Comparación a Colombia, con unas estrategias definidas y reguladas.

Mientras que la tabla 7, detalla las iniciativas que Colombia ha emprendido en el tema de ciberseguridad y cibernética, los cuales aún son prematuras en comparación a los demás países, pero que tras identificar la importancia de proteger este sector por el bien de la soberanía y los ciudadanos el tema ha cobrado mayor relevancia para el estado colombiano.

Tabla 11 Avances de Colombia en ciberseguridad y cibernética

Entidad	Nivel de acción	Dependencia institucional	Capacidades y fortalezas	Limitaciones o desafíos
Dirección de Ciberseguridad y Ciberdefensa del Ejército Nacional (2016)	Táctico-operacional (militar)	Comando del Ejército Nacional (Centro de Entrenamiento y Capacitación del Ejército CATE)	Personal capacitado en seguridad ofensiva y defensiva. Coordinación con el Comando Cibernético. Enfoque militar disciplinado (Ejército Nacional de Colombia, 2023).	Exige mayor inversión tecnológica. Limitado alcance organizacional. Baja visualización pública de sus capacidades. (Ejército Nacional de Colombia, 2023).
Comando Conjunto Cibernético (CCOC) (2013)	Estratégico-conjunto (militar)	Comando General de las Fuerzas Militares	Dirección doctrinal en defensa cibernética conjunta. Capacidad de respuesta ante ciberamenazas híbridas. Participación en ejercicios internacionales (Ejército Nacional de Colombia, 2023).	Falta de interoperabilidad con organismos civiles. Necesidad de integración fluida con el MinTIC y ColCERT (Ejército Nacional de Colombia, 2023).
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) (2020)	Político-normativo (civil)	Rama Ejecutiva Nivel nacional	Conexión con el sector privado y la ciudadanía. Articulación normativa interministerial. Enfoque en infraestructura crítica (Díaz y Cremades, 2024).	Brechas en articulación técnica con el sector defensa Dificultades en alcance territorial y formación regional (Díaz y Cremades, 2024).

ColCERT (Grupo Nacional de Respuesta a Emergencias Cibernéticas) (2013)	Técnico-operativo (civil)	Dirección de Gobierno Digital – MinTIC	Conocido en la región como CERT nacional. Capacidad de respuesta rápida en sectores como salud y energía (ColCERT, 2023).	Aún en consolidación técnica. Dependiente de información sectorial para actuar eficazmente (ColCERT, 2023).
Centro Cibernético Policial (DIJIN – Policía Nacional) (2011)	Investigativo-operativo (policial)	Dirección de Investigación Criminal e INTERPOL (DIJIN)	Extensa experiencia en persecución de cibercriminales. Interacción con INTERPOL y Europol. Infraestructura forense digital (Secretaría de seguridad, convivencia y justicia, 2024).	Enfoque penal, no estratégico. Requiere mayor interoperabilidad con CSIRT del MinTIC. (Secretaría de seguridad, convivencia y justicia, 2024).
Comisión Intersectorial de Seguridad Digital (CISD) (2016)	Conexión institucional	Presidencia de la República (liderada por MinTIC)	Espacio de integración multisectorial. Participación de Defensa, MinDefensa, Superfinanciera, MinSalud, etc. (Departamento Nacional de Planeación, 2020).	Bajo nivel de implementación de decisiones. Funciones más consultivas que ejecutivas. (Departamento Nacional de Planeación, 2020).

Fuente: elaboración propia en base a los autores Díaz y Cremades, 2024; Departamento Nacional de Planeación, 2020; Ejército Nacional de Colombia, 2023; Secretaría de seguridad, convivencia y justicia, 2024 y ColCERT, 2023.

La estructura institucional de ciberseguridad y ciberdefensa en Colombia presenta avances notables en términos de cobertura sectorial, habilidad técnica y desarrollo normativo; sin embargo, aún se manifiesta limitaciones sistemáticas en la coordinación interinstitucional, interoperabilidad civil-militar y consolidación doctrinal. Mientras entidades como el Comando Conjunto Cibernético y la Dirección de Ciberseguridad del Ejército han avanzado en capacidades tácticas y estratégicas en el ámbito militar, su

coordinación con organismos civiles como MinTIC, ColCERT y la CISD resulta escasa para asegurar una respuesta integral frente a amenazas complejas. De igual forma, la existencia de múltiples niveles de acción sin una gobernanza digital unida impide consolidar una estrategia nacional e internacional robusta.

Conclusiones

El análisis comparado de las capacidades tecnológicas, doctrinales y operacionales de Ciberdefensa de los ejércitos de Estados Unidos y Rusia faculta comprender la manera en que las potencias globales preparan sus infraestructuras de protección digital frente a un entorno internacional pronunciado por la intensificación de amenazas híbridas, la ampliación del ciberespionaje y la sofisticación de los ataques orientados a estructuras esenciales.

En primer lugar, la identificación de las capacidades tecnológicas y tácticas expone que ambos países han desarrollado mecanismos cibernéticos de carácter ofensivo-defensivo con alto nivel de integración militar. Estados Unidos, a través del United States Cyber Command (USCYBERCOM) y la Agencia de Seguridad Nacional (NSA), ha fortalecido una estructura interoperable con altos estándares de automatización, inteligencia artificial y defensa activa (CISA, 2024). Por su parte, Rusia ha operado con una fuerte centralización bajo el control del FSB y unidades militares especializadas, como el GTsSI (Glavnoe Upravlenie Spetsialnoy Svyazi i Informatsii), con capacidades de vanguardia en guerra informativa, ciberespionaje y sabotaje digital (Ruiz, 2025).

En segundo lugar, al comparar las políticas nacionales de Ciberdefensa, se muestra que Estados Unidos posee un planteamiento dirigido a la protección de activos civiles y

militares a través de marcos normativos como la National Cyber Strategy (CISA, 2023), que vincula la prevención, detección y respuesta desde un enfoque federal y de cooperación internacional. Rusia, en cambio, prioriza una lógica de "soberanía digital", basada en la autonomía tecnológica (Runet), el control estatal del flujo informativo y la disuasión mediante capacidades ofensivas encubiertas, lo cual limita la transparencia y dificulta la cooperación multilateral (González, 2025).

En tercer lugar, el estudio de incidentes cibernéticos relevantes, como SolarWinds, Microsoft Exchange Server Exploits, el Colonial Pipeline Attack en EE. UU., y el caso de NotPetya, los ciberataques a Ucrania y el Bundestag alemán por parte de Rusia, expone cómo la reacción a las amenazas ha estado subordinada por las capacidades institucionales de cada país. Mientras Estados Unidos ha fortalecido la coordinación interagencial y el trabajo mancomunado con aliados de la OTAN y el sector privado (Adler, 2025), Rusia ha realizado contraataques informativos y medidas de contención interna, pero ha mostrado limitaciones en la protección de sus activos frente a actores como Anonymous o el IT Army of Ukraine (Roccatello y Knight, 2025).

A partir de esta comparación, se precisan fortalezas viables en el contexto colombiano, entre las que se destacan: 1) La necesidad de reforzar una doctrina nacional de Ciberdefensa articulada al sector defensa, en las que ya han ejecutado actividades primitivas; 2) El desarrollo de un Comando Cibernético militar operativo e interoperable; 3) El fortalecimiento de la resiliencia de infraestructuras críticas; 4) La articulación civil-militar en ciberseguridad; y 5) La promoción de una política pública que mezcle defensa activa, protección de datos e integración regional.

En síntesis, la comparación entre Estados Unidos y Rusia muestra que ambos países han desarrollado estrategias de ciberdefensa con ventajas distintas. Estados Unidos insiste por un enfoque institucionalizado y cooperativo, aterrizado en la integración civil-militar, la colaboración con el sector privado y las alianzas internacionales; mientras que Rusia resalta su capacidad de centralización, su rapidez de réplica y el uso amplio de la ciberinteligencia como herramienta estratégica.

A partir de estas experiencias, se propone un modelo híbrido de ciberdefensa adaptado al contexto colombiano, que integre fortalezas de ambos enfoques. Dicho modelo debería considerar:

1. *Centralización operativa con coordinación multisectorial*: reforzar el Comando Conjunto Cibernético de las Fuerzas Militares con una articulación minuciosa con MinTIC, ColCERT y el sector privado.
2. *Defensa activa y resistente*: aplicar doctrinas de anticipación y disuasión como defensa anticipada a través de simulaciones, ejercicios internacionales y cooperación con aliados estratégicos.
3. *Soberanía tecnológica gradual*: impulsar la investigación nacional y el desarrollo de capacidades propias en áreas como criptografía, inteligencia artificial y protección de infraestructuras críticas, minimizando la dependencia en exceso de proveedores externos, pero sin repetir un modelo de aislamiento digital como el ruso.
4. *Alianzas estratégicas y cooperación internacional*: fortalecer la participación en instancias regionales y globales (OEA, OTAN en ejercicios, CSIRT Américas),

beneficiándose del intercambio de información y la construcción de capacidades conjuntas.

5. *Educación y formación especializada*: profundizar en programas académicos y técnicos que preparen talento humano en ciberseguridad y ciberdefensa, asegurando la sostenibilidad de las capacidades conseguidas.

En conclusión, la adopción de este modelo híbrido permitiría a Colombia combinar la capacidad estructural y preventiva estadounidense con la velocidad de respuesta y centralización rusa, creando una doctrina de ciberdefensa integral y flexible. Entendiendo que la ciberdefensa actual no se limita a la tecnología o a la vigilancia, sino que establece un elemento esencial en la seguridad nacional, la proyección geopolítica y la soberanía estatal; lo cual exige a Colombia un reto firme por la institucionalización, la cooperación y la innovación tecnológica en el dominio cibernético.

Referencias

Adler, K. (2025). Por qué la cumbre de la OTAN en Países Bajos puede ser "la más importante desde el fin de la Guerra Fría". *BBC*. https://www.bbc.com/mundo/articles/c5yk2qjv7kvo

Antonio, L. (2025). Future U.S. Cyber Readiness Will Involve Collaboration, Training and Innovation. https://www.afcea.org/signal-media/cyber-edge/future-us-cyber-readiness-will-involve-collaboration-training-and

Arias, R. y Manzano, L. (2023). *El terrorismo y su transformación*. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/download/2938/2404&ved=2ahUKEwib0ZP9ipSNAxXTVTABHcXUKCAQFnoECB4QAQ&usg=AOvVaw15pNdoaejP3gpMW5e77ZFR

Agencias Externas. (2024). Ciberespacio, el campo de batalla de la era tecnológica. https://www.tecnonews.info/noticias/geopolitica_y_ciberespacio_el_nuevo_campo_de_batalla_de_las_naciones

Angarita, J. y Díaz, C. (2020). Modelos epistémicos, investigación y método. Revistas *Universidad Metropolitana de Educación, Ciencia y Tecnología.* https://revistas.umecit.edu.pa/index.php/oratores/article/view/416

Brodowicz, M. (2024). *El impacto de la tecnología en el crecimiento económico y desarrollo de los países en vías de desarrollo*. https://aithor.com/essay-examples/el-

impacto-de-la-tecnologia-en-el-crecimiento-economico-y-desarrollo-de-los-paises-en-vias-de-desarrollo

CISA. (Agencia de Seguridad de Infraestructura y Ciberseguridad). (2022). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*. Cybersecurity y Infrastructure. https://www-cisa-gov.translate.goog/news-events/cybersecurity-advisories/aa22-110a?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

CISA. (Agencia de Seguridad de Infraestructura y Ciberseguridad). (2023). *CISA Plan Estratégico de Ciberseguridad 2023 – 2025*. https://www.cisa.gov/cybersecurity-strategic-plan

CISA. (Agencia de Seguridad de Infraestructura y Ciberseguridad). (2024). *Agentes patrocinados por el estado de la PCR comprometen y mantienen un acceso persistente en las infraestructuras críticas de los EE. UU.* https://www.cisa.gov/sites/default/files/2024-10/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3_ES.pdf

CSIS (Center for Strategic and International Studies). (2025). *Significant Cyber Incidents*. https://www-csis-org.translate.goog/programs/strategic-technologies-program/significant-cyber-incidents?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

ColCERT. (2023). *Política Nacional de Confianza y Seguridad Digital.* https://www.colcert.gov.co/800/w3-channel.html

Cybercom. (2023). *Our mission and vision of USCYBERCOM*. https://www.cybercom.mil/About/Mission-and-Vision/

D´Cunha, S., Rodenhäuser, T. y Ferraro, T. (2025). *"Amenazas híbridas", "zonas grises", "competencia" e "intermediarios": ¿Cuándo hablamos de guerra?* https://blogs.icrc.org/law-and-policy/es/2025/01/28/amenazas-hibridas-zonas-grises-competencia-e-intermediarios-cuando-hablamos-de-guerra/

Departamento Nacional de Planeación. (2020). *Documento CONPES 3995 Política Nacional de Confianza y Seguridad Digital*. https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Díaz, M., y Cremades, A. (2024*).* Revisión del estado actual de la ciberseguridad en Colombia. *Revista Estudios en Seguridad y Defensa*, *19(38), 179-203.* https://doi.org/10.25062/1900-8325.1999

Ejército Nacional de Colombia. (2023). *Plan Estratégico de Transformación Ejército del Futuro 2042. https://www.ejercito.mil.co/plan-estrategico-de-transformacion-ejercito-del-futuro-2042/*

Expósito, J. (2021). La disuasión en el ciberespacio. *Revista Digital sobre Defensa, Armamento y Fuerzas Armadas.* https://www.revistaejercitos.com/focus/ciberdefensa/la-disuasion-en-el-ciberespacio/

Fortune Business Insights. (2025). *Estrategias inteligentes, dando velocidad a su trayectoria de crecimiento 2019-2032*. https://www.fortunebusinessinsights.com/es/u-s-cyber-security-market-107436

González, S. (2025). Israel vs. Irán amenaza regional. *Revista Especializada 16 al 30 de agosto 2025 No. 33*. https://nuevageopolitica.com/PDFS/Revista.pdf

Hassan, Z., Haroon, H., Khalid, A., y Ghayoor, S. (2024). Guerra Digital la evolución de las estrategias de ciberseguridad de Estados Unidos y Rusia. *Vol. 7, (4) 2024, 335-349.* https://real.spcrd.org/index.php/real/article/view/386

ITU (International Telecommunication Union). (2024). *Global Cybersecurity Index*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kristiansen, M. (2021). *Russian Cyber Strategy - Implications for the West*. https://www.stratagem.no/russian-cyber-strategy-implications-for-the-west/

Martin, N. (2022). *Cómo el ciberespacio se ha convertido en el nuevo campo de batalla de la guerra moderna*. https://lc.cx/7ME1Eo

Mogollón, W. G. (2021). Parametrización de lineamientos y políticas para la constitución de un equipo de respuesta a incidentes de seguridad informática CSIRT en el sector agricultura de Colombia. *Escuela Superior de Guerra "General Rafael Reyes Prieto"*. https://www.esdegrepositorio.edu.co/handle/20.500.14205/11069

National Institute of Standards and Technology. (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

NATO. (2024). *Cyber Defense NATO Resources*. https://natolibguides.info/cyberdefence

Niss, O. (2023). *La Ciberdefensa ofensiva y la inteligencia artificial. In Simposio Argentino de Informática y Derecho (SID 2023)-JAIIO 52*. Universidad Nacional de Colombia. https://sedici.unlp.edu.ar/handle/10915/165477

Nobrega, K., Rutkowski, A. y Saunders, C. (2024). *The whole of cyber defense: Syncing practice and theory*. https://www-sciencedirect-com.translate.goog/science/article/pii/S096386872400043X?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

OEA (Organización de Estados Americanos). (2023). *Guía práctica para CSIRTs*. Volumen 2. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

Ortega, C. (2023). *¿Qué es el muestreo por conveniencia?* https://www.questionpro.com/blog/es/muestreo-por-conveniencia/

Patino, G. (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. *Revista Externado.* https://revistas.uexternado.edu.co/index.php/oasis/article/view/7166

Pringle, R. (2025). *Federal Security Service Russian government agency*. https://www-britannica-com.translate.goog/topic/Federal-Security-Service

Ramírez, N. (2021). Ciberresilencia. *Revista Sistemas ACIS*. https://sistemas.acis.org.co/index.php/sistemas/article/view/155

Rivera, L. y Hernández, S. (2023). La ciberseguridad un enfoque de aprendizaje, desde el rol del suboficial del Ejército Nacional de Colombia. *Revista Miradas Vol. 18 Núm. 2.* https://revistas.utp.edu.co/index.php/miradas/article/view/25519

Roccatello, A. y Knight, A. (2025). *La verdad en Ucrania en medio de una desinformación generalizada y un sistema internacional debilitado*. https://www.ictj.org/es/%C3%BAltimas-noticias/la-verdad-en-ucrania-en-medio-de-una-desinformaci%C3%B3n-generalizada-y-un-sistema

Rodeheffer, L. (2025). *Russia Ramps Up Cybersecurity Systems*. https://jamestown-org.translate.goog/program/russia-ramps-up-cybersecurity-systems/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Rodríguez, J. (2022). Análisis de la ciberdefensa y ciberseguridad en la seguridad Ciudadana en Bogotá. *Universidad Militar Nueva Granada.* https://lc.cx/OwsJuq

Ruiz, V. (2025). *Alertan por aumento de ciberataques que explotan vulnerabilidades de software en infraestructura crítica*. https://www.infobae.com/mexico/2025/05/31/alertan-por-aumento-de-ciberataques-que-explotan-vulnerabilidades-de-software-en-infraestructura-critica/

Secretaría de seguridad, convivencia y justicia. (2024). *Centro Cibernético del Gaula: tecnología contra la extorsión en Bogotá*. https://scj.gov.co/es/noticias/centro-cibern%C3%A9tico-del-gaula-tecnolog%C3%ADa-contra-la-extorsi%C3%B3n-bogot%C3%A1

Secureframe. (2024). *130+ Estadísticas de Ciberseguridad para Inspirar Acción Este Año*. https://secureframe.com/es-es/blog/cybersecurity-statistics

Seitz, K. (2024). *Explorando el papel vital de la ciberseguridad en el ámbito militar: aplicaciones, tecnologías y capacitación*. https://www-lighthouselabs-ca.translate.goog/en/blog/cybersecurity-in-the-military?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Urbina, E. (2020). Investigación cualitativa*. Applied Sciences in Dentistry. 1(3).* https://rhv.uv.cl/index.php/asid/article/download/2574/2500

Verdugo, J. (2020). El escenario híbrido y su impacto en el nivel de la conducción operacional. Capítulo 3. file:///C:/Users/hp/Downloads/144-Texto%20del%20art%C3%ADculo-181-1-10-20210811.pdf

Zambrano, A. F. (2022). Política pública de ciberdiplomacia en Colombia para contener las amenazas a la Ciberdefensa. *Escuela Superior de Guerra "General Rafael Reyes Prieto".* https://www.esdegrepositorio.edu.co/handle/20.500.14205/11160