Ensayo

Entre el código y la soberanía:

la ciberdefensa argentina frente al desafío de las infraestructuras críticas

Between Code and Sovereignty:

Argentine Cyber Defense and the Challenge of Critical Infrastructures

FIDEL AGUSTÍN ASCONA

Universidad Nacional Madres de Plaza de Mayo (UNMa), Argentina

asconafidel@gmail.com

Resumen

Este ensayo examina el lugar que ocupa la ciberdefensa en la agenda estratégica argentina a partir de su evolución normativa, institucional y doctrinaria reciente. Se parte de una hipótesis central: en el escenario contemporáneo la ciberdefensa ya no puede ser concebida como un apéndice técnico de las comunicaciones militares, sino como una dimensión transversal del planeamiento, la protección de infraestructuras críticas y la preservación de la soberanía. Sobre esa base, se analiza la definición adoptada por el Ministerio de Defensa, la consolidación del Comando Conjunto de Ciberdefensa, la creación del Centro Nacional de Ciberdefensa y la necesidad de articular capacidades militares, industria, sistema científico y formación especializada. El trabajo sostiene que la principal dificultad argentina no reside únicamente en la amenaza externa, sino también en la fragmentación de capacidades, la dependencia tecnológica y la escasez de recursos humanos altamente calificados. Finalmente, se propone una agenda de fortalecimiento orientada a la acción conjunta, la doctrina, la resiliencia de los sistemas críticos y la construcción de autonomía tecnológica compatible con el marco jurídico nacional.

Abstract

This essay examines the place of cyber defence in Argentina's strategic agenda through its recent normative, institutional, and doctrinal evolution. It starts from a central hypothesis: in the current environment, cyber defence can no longer be understood as a merely technical extension of military communications, but rather as a cross-cutting dimension of planning, critical infrastructure protection, and sovereignty preservation. On that basis, the article analyses the definition adopted by the Ministry of Defence, the consolidation of the Joint Cyber Defence Command, the creation of the National Cyber Defence Centre, and the need to articulate military capabilities with industry, the scientific system, and specialised education. It argues that Argentina's main difficulty lies not only in external threats but also in fragmented capabilities, technological dependence, and the shortage of highly qualified personnel. Finally, it proposes a strengthening agenda focused on joint action, doctrine, resilience of critical systems, and the development of technological autonomy compatible with the national legal framework.

Palabras clave: ciberdefensa, defensa nacional, infraestructuras críticas, soberanía tecnológica, planeamiento conjunto.

Keywords: Cyber defence, national defence, critical infrastructure, technological sovereignty, joint planning.

Introducción

La transformación digital de la vida estatal, económica y militar modificó de manera profunda la discusión clásica sobre la defensa nacional. El ciberespacio dejó de ser un ámbito auxiliar de apoyo técnico para convertirse en un entorno donde se disputan información, disponibilidad operativa, continuidad logística, capacidad de mando y libertad de acción. En otras palabras, la dimensión cibernética atraviesa hoy funciones que antes se pensaban por separado: comunicaciones, inteligencia, comando y control, producción industrial, infraestructura energética, transporte y sistemas de armas.

En la Argentina, esta mutación plantea un problema singular. A diferencia de otros países que adoptaron marcos más difusos entre defensa, seguridad interior e inteligencia, el ordenamiento argentino conserva una diferenciación orgánica y funcional que responde a su experiencia histórica y a decisiones normativas precisas. Por ello, el problema no consiste solamente en "sumar tecnología", sino en definir con claridad qué corresponde a la defensa, qué compete a la ciberseguridad civil y cómo se articulan ambas esferas, sin desdibujar límites jurídicos relevantes (Ley 23.554, 1988; Ley 24.059, 1992; Ley 25.520, 2001).

Este trabajo sostiene que la ciberdefensa constituye hoy una capacidad estratégica del instrumento militar argentino y que su consolidación exige superar una visión meramente técnica. La tesis que aquí se propone es que la principal tarea pendiente no es sólo adquirir herramientas o plataformas, sino integrar doctrina, organización, formación, planeamiento y desarrollo tecnológico nacional en una arquitectura coherente. Para demostrarlo, primero se reconstruye el encuadre conceptual y normativo vigente; luego se examina la arquitectura institucional actual; finalmente, se analizan los desafíos principales y se propone una agenda de fortalecimiento de mediano plazo.

Delimitación conceptual y encuadre normativo

La cuestión conceptual es decisiva porque, en materia cibernética, las palabras ordenan competencias, recursos y responsabilidades. Una definición demasiado amplia puede diluir el papel específico del instrumento militar; una definición demasiado estrecha, en cambio, puede volver inútiles las capacidades desarrolladas. Por ello, la literatura argentina especializada ha insistido en que la ciberdefensa debe ser pensada dentro del sistema de defensa, pero en diálogo con problemas más amplios de soberanía, infraestructura crítica y dependencia tecnológica (Ocón y Gastaldi, 2019; Eissa y Albarracín Keticoglu, 2020).

El marco jurídico nacional ofrece un primer criterio ordenador. La Ley de

Defensa Nacional fija que la defensa se orienta a la preparación y ejecución de acciones frente a agresiones de origen externo. La Ley de Seguridad Interior, por su parte, regula otro campo institucional, y la Ley de Inteligencia Nacional impone límites adicionales al empleo de capacidades estatales sobre personas, grupos u organizaciones del ámbito interno. En consecuencia, la incorporación de la dimensión cibernética no puede ignorar esa arquitectura previa, sino que debe adaptarse a ella (Ley 23.554, 1988; Ley 24.059, 1992; Ley 25.520, 2001).

Un punto de inflexión importante se produjo con la evolución doctrinaria y normativa de la última década. La Resolución 1380/2019 del Ministerio de Defensa redefinió la ciberdefensa como las acciones y capacidades desarrolladas por el Ministerio de Defensa, el Estado Mayor Conjunto y las Fuerzas Armadas para anticipar y prevenir ciberataques y ciberexplotación de redes que puedan afectar al ministerio, al instrumento militar y a infraestructuras críticas operacionales soporte de servicios esenciales de interés para la defensa o de procesos industriales sensibles para ella (Ministerio de Defensa, 2019). La importancia de esa formulación radica en dos aspectos: en primer lugar, desplaza la mirada desde la informática aislada hacia la protección de funciones estratégicas. En segundo lugar, incorpora explícitamente la defensa de activos digitales y de infraestructuras críticas asociadas al sector defensa.

Esta redefinición no surgió en el vacío. Como demostraron Eissa y Albarracín Keticoglu (2020), la discusión argentina sobre ciberdefensa estuvo marcada por tensiones sobre su ubicación institucional, por la dificultad de traducir al plano local modelos importados y por el riesgo permanente de confundir defensa con seguridad interior. De allí que el debate argentino tenga una densidad política particular: discutir ciberdefensa no equivale simplemente a debatir software, sino a redefinir la relación entre soberanía, tecnología y empleo legal de la fuerza.

El Libro Blanco de la Defensa 2023 retoma este problema en una clave más amplia al presentar la transformación tecnológica como uno de los factores decisivos del escenario estratégico contemporáneo. Allí, la ciberdefensa aparece vinculada al planeamiento por capacidades, a la protección de infraestructuras críticas y a la necesidad de fortalecer la acción conjunta del instrumento militar (Ministerio de Defensa, 2023). Esa lectura resulta correcta: la defensa del ciberespacio relevante para la defensa nacional no puede resolverse por mera agregación de herramientas, sino a través de una lógica de sistema.

La arquitectura institucional actual

La institucionalización de la ciberdefensa argentina muestra avances concretos que conviene valorar, sin caer en diagnósticos complacientes. La Resolución 1380/2019 creó el Centro Nacional de Ciberdefensa en el ámbito de la Subsecretaría de Ciberdefensa, concentrando allí el CSIRT de Defensa, el centro inteligente de operaciones de seguridad del Comando Conjunto de Ciberdefensa y el laboratorio de análisis cibernético, entre otras plataformas (Ministerio de Defensa, 2019). Esa decisión buscó resolver un problema clásico: la dispersión de capacidades entre áreas administrativas, técnicas y operacionales. En el plano operacional, el propio Comando Conjunto de Ciberdefensa define entre sus funciones la protección de las redes informáticas de la defensa y, a orden, de las infraestructuras críticas que se le asignen (Estado Mayor Conjunto de las Fuerzas Armadas, 2024).

A la vez, la persistencia y jerarquización del Comando Conjunto de Ciberdefensa dentro de la estructura militar conjunta constituye un indicador de maduración institucional. La reglamentación del Sistema de Defensa Nacional aprobada por el Decreto 1112/2024 incluye expresamente al Comando Conjunto de Ciberdefensa entre los comandos conjuntos permanentes que operan en tiempos de paz dentro de los espacios de la defensa nacional (Poder Ejecutivo Nacional, 2024). La norma no lo presenta como un agregado accesorio, sino como parte de la arquitectura permanente del instrumento militar, junto con otros comandos vinculados al control aeroespacial, marítimo, antártico y de operaciones especiales.

Este punto es central. Si la organización revela prioridades estratégicas, la presencia del comando ciber en la estructura conjunta indica que la dimensión digital dejó de ser concebida como soporte subordinado para convertirse en una capacidad operativa estable. La existencia de un Instituto de Ciberdefensa en el ámbito del Estado Mayor Conjunto, visible incluso en la estructura pública de autoridades, refuerza además la idea de que la formación, la doctrina y la producción de conocimiento son componentes inseparables del problema (Estado Mayor Conjunto de las Fuerzas Armadas, 2024).

Sin embargo, la institucionalización no equivale por sí misma a una solución acabada. Taverna y Rutz (2021) advirtieron que el desarrollo de infraestructuras críticas de la información exige no solo organización burocrática, sino también gestión de riesgos, coordinación interinstitucional, actualización permanente y formación especializada. La experiencia internacional reciente confirma esta observación: los incidentes cibernéticos relevantes rara vez afectan un solo sistema aislado, tienden más bien a comprometer cadenas logísticas, redes de proveedores, servicios tercerizados y procesos industriales interdependientes. Por eso, la arquitectura institucional solo resulta eficaz si logra traducirse en procedimientos, ejercicios, interoperabilidad y capacidad real de respuesta.

Los desafíos de la ciberdefensa argentina en la actualidad

El primer desafío es doctrinario. La Argentina dispone hoy de mejores definiciones y de una estructura más visible que hace una década, pero aún debe consolidar una doctrina verdaderamente integrada sobre empleo, prevención, resiliencia y recuperación. No se trata únicamente de responder a un ataque consumado. La cuestión central consiste en preservar la disponibilidad operativa de sistemas, sostener la cadena de mando y reducir vulnerabilidades antes de que el incidente produzca efectos tácticos, operacionales o estratégicos. En este punto, la ciberdefensa debe ser comprendida como una función transversal del planeamiento, no como una especialidad autónoma aislada del resto de las operaciones.

El segundo desafío es la protección de infraestructuras críticas. La normativa de 2019 ya había advertido que la ciberdefensa debe abarcar tanto infraestructuras operacionales soporte de servicios esenciales de interés para la defensa como procesos industriales sensibles vinculados a la fabricación de bienes estratégicos (Ministerio de Defensa, 2019). Ello introduce una consecuencia práctica de gran importancia: la agenda de defensa digital no termina en los cuarteles ni en los centros de datos militares. Se extiende hacia empresas, laboratorios, organismos técnicos, proveedores y redes logísticas cuya afectación puede degradar la capacidad defensiva del Estado.

El tercer desafío es el capital humano: Rutz (2020) mostró que la formación de posgrado en ciberdefensa y ciberseguridad en la Argentina es aún insuficiente frente a la magnitud del problema. Esa observación mantiene vigencia. La escasez de especialistas no se corrige exclusivamente con cursos breves ni con compras de equipamiento. Requiere una política sostenida de formación, retención y actualización profesional. Más todavía: exige construir trayectorias que combinen conocimientos técnicos, comprensión estratégica, nociones jurídicas y cultura conjunta. Un analista brillante en seguridad informática que desconozca el funcionamiento del sistema de defensa puede ser tan limitado como un cuadro militar sobresaliente que no comprenda la lógica técnica del entorno digital.

El cuarto desafío es la dependencia tecnológica: Ocón y Gastaldi (2019) señalaron que la discusión sobre ciberespacio y soberanía no puede separarse de la autonomía tecnológica. En defensa, esta observación resulta especialmente pertinente. Cuanto mayor es la dependencia respecto de *hardware*, *software*, servicios en la nube o cadenas de actualización controladas desde el exterior, mayor es también la vulnerabilidad estructural. La soberanía tecnológica no implica autarquía absoluta ni rechazo irracional de la cooperación internacional, significa, más bien, capacidad propia para comprender, auditar, adaptar, operar y proteger sistemas críticos sin depender enteramente de decisiones ajenas.

El quinto desafío es la articulación entre ciberdefensa y ciberseguridad

nacional. La existencia de una Dirección Nacional de Ciberseguridad y del CERT.Ar muestra que el Estado argentino desarrolló también capacidades civiles en esta materia (Jefatura de Gabinete de Ministros, 2021). Esa evolución es positiva, pero obliga a coordinar mejor sin confundir planos. La ciberseguridad protege, entre otras cosas, servicios civiles, administración pública y entornos digitales generales del Estado. La ciberdefensa, en cambio, se concentra en aquello que compromete la defensa nacional y el instrumento militar. La articulación debe existir; la superposición indiferenciada, no.

Por último, existe un desafío político-institucional más amplio: sostener continuidad. La experiencia argentina demuestra que muchas capacidades estratégicas se resienten cuando dependen en exceso de orientaciones coyunturales o de liderazgos circunstanciales. La ciberdefensa necesita políticas de Estado relativamente estables, presupuesto sostenido, vínculos duraderos con universidades, sistema científico e industria, y un marco de evaluación institucional que permita corregir desvíos sin reiniciar el proceso en cada cambio de gestión.

Una agenda de fortalecimiento para el mediano plazo

Si la ciberdefensa es una dimensión estructural de la defensa nacional, entonces su fortalecimiento no puede quedar reducido a compras aisladas o a respuestas reactivas frente a incidentes. Se requiere, por el contrario, una agenda articulada en al menos cinco direcciones.

La primera consiste en profundizar la doctrina conjunta. El Comando Conjunto de Ciberdefensa debe seguir siendo el espacio privilegiado para consolidar procedimientos comunes, ejercicios y estándares de interoperabilidad entre las Fuerzas Armadas. La acción conjunta, en este terreno, no es una preferencia organizacional sino una necesidad operativa. Las amenazas y vulnerabilidades no distinguen entre componentes terrestres, navales, aéreos o espaciales; por lo tanto, la respuesta tampoco debería hacerlo.

La segunda dirección es la protección efectiva de infraestructuras críticas vinculadas a la defensa. Ello exige identificar dependencias estratégicas, auditar vulnerabilidades, definir niveles de criticidad y establecer protocolos de redundancia, segmentación y recuperación. La resiliencia debe ser medida no solo por la capacidad de bloquear un ataque, sino también por la rapidez y confiabilidad con que el sistema puede volver a operar.

La tercera es la formación de recursos humanos. La experiencia argentina ya produjo antecedentes valiosos de posgrado y reflexión académica en la materia (Rutz, 2020; Taverna y Rutz, 2021). El paso siguiente debería ser consolidar una política más amplia que articule institutos militares, universidades públicas, sector científico-tecnológico y programas específicos de investigación aplicada. Formar personal en ciberdefensa no significa solo

enseñar herramientas, significa producir criterio profesional para actuar en un terreno donde convergen estrategia, derecho, tecnología y conducción.

La cuarta dirección es el desarrollo tecnológico nacional. La defensa no puede depender de manera absoluta de soluciones cerradas cuya arquitectura, actualización o vulnerabilidades reales se definan fuera del control estatal. Promover capacidades nacionales en criptografía aplicada, monitoreo, análisis de vulnerabilidades, simulación, entrenamiento y componentes críticos no es un lujo doctrinario, sino una condición de autonomía. En este punto, la vinculación con CITEDEF, universidades y empresas tecnológicas nacionales adquiere un valor estratégico evidente.

La quinta dirección es la coordinación con otros organismos del Estado. La diferenciación jurídica entre defensa, seguridad interior e inteligencia no debe convertirse en aislamiento institucional. La coordinación con áreas civiles de ciberseguridad, con organismos de respuesta a incidentes y con sectores reguladores de infraestructuras estratégicas debe realizarse con reglas claras, competencias precisas y canales permanentes de intercambio. El desafío argentino no es copiar modelos externos, sino construir una articulación propia compatible con su diseño constitucional y legal.

En síntesis, una política seria de ciberdefensa requiere continuidad, gradualidad y densidad institucional. No será el resultado de una sola norma ni de un solo plan, sino de una acumulación persistente de capacidades.

Conclusión

La ciberdefensa ya forma parte del núcleo duro de la defensa nacional. En la Argentina, su desarrollo reciente muestra avances relevantes: una definición más precisa, una estructura conjunta visible, instrumentos institucionales específicos y una creciente producción académica local. Sin embargo, el problema está lejos de resolverse. Persisten déficits doctrinarios, fragmentación de capacidades, dependencia tecnológica y escasez de personal altamente especializado.

El punto decisivo es comprender que la ciberdefensa no debe ser tratada como una moda tecnológica ni como un asunto meramente informático. En ella convergen soberanía, organización estatal, infraestructura crítica, industria estratégica y planeamiento militar. Por eso, su fortalecimiento demanda una política sostenida que combine marco jurídico, conducción estratégica, formación y desarrollo tecnológico nacional.

La Argentina no parte de cero. Cuenta con experiencia normativa, con antecedentes institucionales y con una comunidad académica que ya produjo reflexiones valiosas. El desafío actual consiste en convertir esos avances en una capacidad verdaderamente integrada, resiliente y compatible con el interés nacional. En el escenario contemporáneo, defender la soberanía también implica defender sistemas, datos, redes, procesos industriales y cadenas de mando. La ciberdefensa, entendida en estos términos, dejó de ser un capítulo secundario para convertirse en una condición de posibilidad de la defensa misma.

Bibliografía

Cornaglia, S. y Vercelli, A. H. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). URVIO. *Revista Latinoamericana de Estudios de Seguridad*, 20, 46-62.

Eissa, S. G. y Albarracín Keticoglu, A. (2020). La ciberdefensa en su laberinto. Cambio de rumbo en la concepción de ciberdefensa durante la gestión de Mauricio Macri (2015-2019). *Defensa Nacional*, 5, 7-41.

Estado Mayor Conjunto de las Fuerzas Armadas. (2024). Función del Comando Conjunto de Ciberdefensa. *Argentina.gob.ar*. https://www.argentina.gob.ar/historia-del-comando-conjunto-de-ciberdefensa/funcion-del-comando-conjunto-de-ciberdefensa.

Ley 23.554 (1988). Ley de Defensa Nacional, República Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-23554-20988/texto.

Ley 24.059 (1992). Ley de Seguridad Interior, República Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-24059-458/texto.

Ley 25.520 (2001). Ley de Inteligencia Nacional, República Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-25520-70496/texto.

Ministerio de Defensa (2019). Resolución 1380/2019. Política de Ciberdefensa. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/219968/20191029.

Ministerio de Defensa (2023). Libro Blanco de la Defensa 2023. https://www.argentina.gob.ar/sites/default/files/2021/11/libroblancodeladefensa2023_.pdf.

Ocón, A. L. y Gastaldi, S. (2019). Ciberespacio y defensa nacional: una reflexión sobre el dilema libertad-seguridad en el ejercicio de la soberanía. *Defensa Nacional*, 2, 88-108.

Presidencia de la Nación (2024). Decreto 1112/2024. Sistema de Defensa Nacional. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/318502/20241220.

Rutz, G. (2020). Ciberdefensa y formación de posgrados en Argentina: reflexiones a partir de perspectivas políticas y sociales para el interés de la soberanía nacional. *Defensa Nacional*, 3, 39-79.

Taverna, A. y Rutz, G. (2021). Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información en Argentina. *Defensa Nacional*, 6, 181-204.