ARI 18/2025
6 de febrero de 2025

El concepto de Ciberdefensa Activa

Félix Arteaga | Investigador principal, Real Instituto Elcano.

Javier Alonso Lecuit | investigador sénior asociado, Real Instituto Elcano.

Tema

Las medidas defensivas públicas y privadas no bastan para contener el crecimiento de los ciberataques. El concepto y las medidas de ciberdefensa activa podrían incrementar la disuasión de España.

Resumen

Los conceptos[1] buscan soluciones a problemas. En el ciberespacio, el problema es que los ciberataques crecen en todos los sectores, públicos y privados, y que los Estados no son capaces de contener la progresión. Se utilizan por los Estados como arma de la confrontación geopolítica y por grupos criminales organizados en colaboración con los anteriores o por su cuenta. Las medidas defensivas no bastan y se precisan medidas disuasorias. El concepto de ciberdefensa activa (CDA) se acuñó para disponer de medidas disuasorias y ofensivas que completaran el espectro entre las defensivas pasivas y las diseñadas para la guerra cibernética. De esta forma, se ampliaba la arquitectura de seguridad tradicional de las organizaciones públicas y privadas a nuevos espacios de respuesta, reservando las capacidades más ofensivas para los gobiernos, pero abriendo las respuestas ofensivas a la corresponsabilidad público-privada. La implantación está rodeada de dificultades conceptuales, normativas y de gestión, por lo que cada Estado adopta su concepto nacional, el marco regulatorio que lo desarrolla y el nivel de ambición de la cooperación público-privada en materia de disuasión.

Análisis

El ciberespacio facilita la acción ofensiva de los atacantes frente a la de los defensores, los ciberataques no paran de crecer y las medidas de seguridad adoptadas se muestran insuficientes para proporcionar niveles de resiliencia tolerables. En el ciberespacio se difuminan las fronteras entre ciberdefensa y ciberseguridad, amenazas externas e internas, paz y guerra, y medidas pasivas y activas, con lo que también se difumina la separación de funciones entre los sectores público y privado.[2] Las tensiones geopolíticas aumentan el número, variedad y efecto de los ciberataques, multiplicando la interacción entre grupos con vinculaciones estatales, activistas, cibercriminales organizados y prestadores o usuarios de servicios. La denominada guerra híbrida afecta

[1] Los autores desean agradecer la colaboración de los miembros del Grupo de Trabajo sobre Ciberpolíticas del Real Instituto Elcano que ambos coordinan.

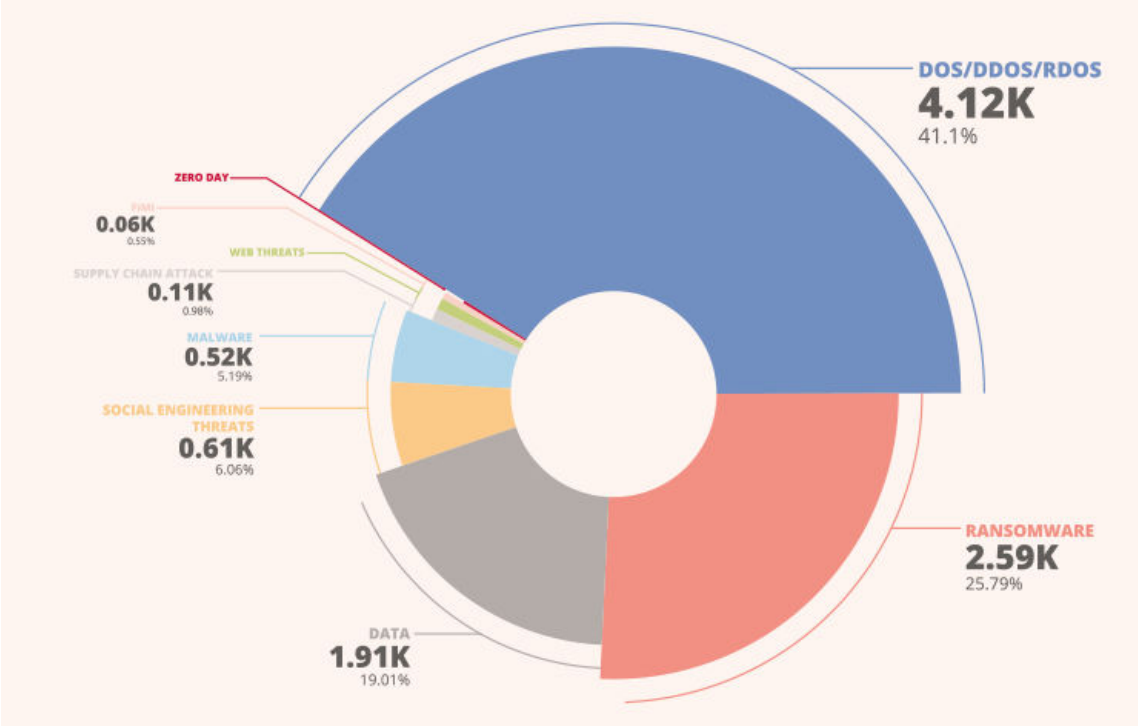
[2] Damjan Strucl (2021), “Comparative study on the cyber defence of NATO Member States”, NATO, CCDCOE, p. 21; Rebeca Slayton (2016), “What is the Cyber offense-Defense Balance”, International Security 41, nº 3.

a operaciones de influencia y ciberataques relacionadas con conflictos, elecciones, sistemas IT y, crecientemente a sistemas OT, de los países occidentales incluida España.

Los ciberataques muestran una deriva geopolítica por la que se atacan objetivos del sector privado como parte de los ataques contra los Estados e instituciones.[3] Junto a los ciberataques patrocinados por los Estados, o por grupos afines a ellos, se ha desarrollado un creciente mercado ilegal (*deep web y dark net*) pero también legal (*access-as-a-service*) de capacidades ofensivas como servicio que facilitan la proliferación de ciberataques.[4] A lo anterior se añaden las limitaciones del derecho internacional para regular el uso responsable de las ciberoperaciones ofensivas (*responsible cyber power*) con el fin de reducir los riesgos asociados a su empleo.

La convergencia de los factores anteriores desborda las capacidades del sector privado y colocan al sector público ante la responsabilidad de ejercer la capacidad coactiva de la que tienen el monopolio para proteger a quienes no la tienen. Los Estados deben proteger o disuadir y las medidas defensivas que emplean no bastan para hacer frente a los incidentes que se registran (Figura 1). Este es el problema al que el concepto de ciberseguridad activa intenta dar respuesta.

Figura 1. Incidentes registrados en la UE entre julio 2023 y junio 2024



Fuente: ENISA.

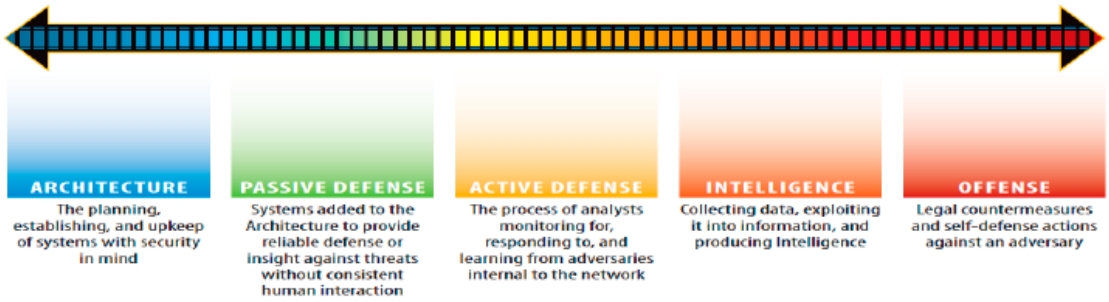
[3] International Chamber of Commerce (2024), "Protecting the cybersecurity of critical infrastructure and their chains of supply", *ICC Working Paper*, julio, p. 6.

[4] Winnona DeSombre y otros (2024), "Countering Cyber Proliferation: Zeroing in on Access-as-a Service", Atlantic Council, 1/III/2024; Louise Marie Hurel y otros (2024), "The Pall Mall Process on Cyber Intrusion", RUSI, 20/II/2024.

La asimetría entre ataques y respuestas se ha tratado de corregir con varios conceptos a lo largo del tiempo. A diferencia de la guerra tradicional de donde procede, el concepto de disuasión no se ha podido aplicar con éxito al ciberespacio en ninguna de sus variantes de denegación (capacidad para contrarrestar los ataques) o de castigo (capacidad para devolverlos).[5] En ambos casos es necesario comunicar la voluntad de disuadir (política declaratoria) y disponer de capacidades creíbles.[6] Conocer si la disuasión funciona o no en el ciberespacio es difícil debido a la naturaleza clasificada de las operaciones ofensivas y la escasez de casos disponibles en fuentes abiertas. En la primera década de este siglo se hizo evidente que las medidas de protección pasiva no funcionaban y Estados Unidos (EEUU) desarrolló una política de defensa activa que permitía llevar a cabo operaciones que produjeran efectos fuera de su territorio para prevenir ataques inminentes bajo control presidencial. Sin embargo, esas medidas *ad hoc* no impidieron ciberataques tan relevantes como los que afectaron a la presa Bowman Avenue de Nueva York, Sony Pictures en 2014, la fuga de datos de la Personnel Management Office en 2015 y la de datos financieros en 2016, los WannaCry, NotPetya de 2017, o sobre el oleoducto Colonial en 2021, entre otros.

La insatisfacción por los resultados condujo a la aparición de nuevos conceptos como los de contacto persistente (*persistent engagement*) y defensa adelantada (*defending forward*).[7] Desde entonces, el concepto de ciberdefensa activa ha evolucionado tanto para reducir sus contraindicaciones como para moderar su ambición. En su creciente implantación influyen el contexto de geopolitización, en el que se prodigan los ciberataques por debajo del umbral de conflicto, y de intrusión, donde proliferan tecnologías que aumentan la frecuencia, el riesgo y la exposición a los ciberataques. La CDA ya se ha integrado en el concepto de ciberseguridad, tal y como representa la Figura 2, en el que se ocupa del análisis monitorización, respuesta y aprendizaje sobre adversarios dentro de propia red.

Figura 2. La escala móvil de la ciberseguridad



Fuente: CCDCOE, 2021.[8]

[5] Joe Burton (2020), "Cyber Deterrence: A Comprehensive Approach? NATO CCD COE.

[6] Marcus Willet (2024), "Cyber Operations and Their Risponsible Use", Adelphi Series, IISS.

[7] U.S. CyberCOM (2022), "CYBER 101 - Defend Forward and Persistent Engagement", 25/II/2022.

[8] Damjan Strucl (2021), "Comparative study on the cyber defence of NATO Member States", CCDCOE, p. 18.

Lo significativo de los conceptos señalados es que las medidas ofensivas, con sus mayores o menores limitaciones, se han ido incorporando a los inventarios públicos de respuesta de la ciberseguridad, la ciberdefensa y la ciberresiliencia frente a los ataques. La superposición de riesgos e instrumentos diluye la separación entre la ciberdefensa, que se consideraba como un ámbito militar, y la ciberseguridad que pertenecería al campo civil, cuando ambos medios desarrollan medidas defensivas pasivas y activas.[9] El contexto de geopolitización e intrusión multiplica los objetivos a proteger en el ciberespacio, tanto para los actores públicos como privados, y se precisa mayor capacidad (*cyber power*) para proporcionar resiliencia a las infraestructuras críticas y las redes, y sistemas de información.[10]

En principio, el sector público es responsable de la regulación y protección del sector privado, por lo que éste sólo puede actuar de forma subsidiaria y en situaciones de legítima defensa. Sin embargo, la demanda por el sector privado de medidas CDA ha crecido ante la incapacidad crónica del sector público para garantizar la protección de las redes y sistemas de información a pesar de las medidas defensivas adoptadas por los actores privados, por lo que desde estos sectores se ha solicitado la regulación o la adopción de esas medidas disuasorias por los gobiernos.[11] El mismo monopolio del poder coactivo que los Estados reivindican para limitar el derecho de autodefensa de los actores privados, principio de subsidiariedad, los obliga a dotarse de capacidades para defenderles.

Las propuestas favorables a la CDA tratan de establecer una regulación y un mercado para las medidas de defensa activa del sector privado, llevando la cooperación público-privada a un nivel superior de corresponsabilidad. No proponen que cualquier actor privado desarrolle ciberoperaciones ofensivas, sino que los Estados aprovechen el potencial del sector privado y certifiquen aquellas empresas privadas que pueden colaborar al desarrollo de la CDA.[12] La "normalización" de la CDA mediante su reconocimiento público (declaración) y su regulación nacional debe acompañarse de un esfuerzo diplomático para que el derecho internacional ampare su "uso responsable". El empleo de contramedidas por los Estados en respuesta a las agresiones de otros está admitido por el derecho internacional, aunque las medidas punitivas que van más allá de la interrupción y reparación de la agresión generan controversias.[13] Las contramedidas "responsables" en el ciberespacio carecen todavía de un marco

[9] Patryk Pawlak y François Delerue (eds.) (2022), "A Language of Power? Cyber defence in the European Union", *EUIIS Chaillot Paper* 176, noviembre, p. 13.

[10] El Reino Unido define poder militar como "la capacidad de proteger y fomentar el interés nacional dentro y a través del ciberespacio", National Cyber Strategy 2022, p. 11.

[11] Barbaby Frumess (2015), "A Definitive Guide to Active Cyber Defense: modularizing cybersecurity", diciembre; Jeremy Rabkin y Ariel Rabkin (2024), "Hacking Back Without Cracking Up", *AEGIS Essays*, Hoover Institution, 28/VI/2024; Felix Arteaga y Javier Alonso (coords.) (2019), "Propuestas desde el sector privado para la revisión de la Estrategia Nacional de Ciberseguridad", *DT* 4/20019, Real Instituto Elcano, p. 6.

[12] Dennis Broeders (2021), "Private active cyber defense and (international) cyber security - pushing the line?", The Hague Program for Cyber Norms, Institute of Security and Global Affairs, Leiden University, 1/III/2021.

[13] Talita Dias (2024), "Countermeasures in international law and their role in cyberspace", *Chatham House Research Paper*, mayo.

consuetudinario que les proporcione cobertura, principalmente porque las ciberoperaciones se desarrollan en un marco encubierto, automatizado y de escalada. La creciente colaboración entre agentes gubernamentales y no gubernamentales en los ataques aumenta la necesidad de integrar recursos, tanto públicos como privados a nivel estatal e intergubernamental. En consecuencia, las fuerzas y cuerpos de seguridad, nacionales e internacionales, también recurren a instrumentos de ciberdefensa activa para combatir la criminalidad organizada, desarrollando lo que la Estrategia de Ciberseguridad belga de 2021 llama "capacidad represiva adecuada" para trascender el ámbito de la investigación policial pasiva, pero sin entrar en el de las operaciones militares.[14] En el mismo sentido, la Estrategia de Ciberseguridad de Australia de 2023 admite el empleo de acciones ofensivas contra los cibercriminales.

Adoptar medidas CDA consiste en acceder a las capacidades tecnológicas para llevar a cabo operaciones ofensivas, independientemente de quién realiza la operación. La limitación de los medios públicos avala la colaboración con el sector privado para crear una base industrial que preserve la autonomía estratégica nacional sobre la base de un mercado reglado de ciberdefensa activa.

1. Definiciones

El concepto y sus variantes han generado numerosas definiciones que dificultan delimitar sus bordes sin que exista todavía una definición aceptada. La de mayor relevancia por su carácter seminal desde 2016 es la del *Center for Cyber & Homeland Security*:[15]

> *"*Active defense is a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors. The term active defense is not synonymous with "hacking back" and the two should not be used interchangeably*".*

Entre las definiciones académicas más conocidas figuran las de Dewar que define la CDA como la "detección, análisis y mitigación proactivos de las violaciones de seguridad de la red en tiempo real combinado con contramedidas agresivas desplegadas fuera de la red de la víctima".[16] Definición que combina los tres paradigmas de ciberseguridad (protección), ciberdefensa (neutralización) y resiliencia (continuidad). Para Sven Harpig, una operación CDA es en la que emplea medidas técnicas y operativas ordenadas por

[14] Gavin Wilde & Emma Landi (2024) "Western Law Enforcement Agencies are Going on the Cyber Offensive", RUSI, 21/VI/2024; Centro de Ciberseguridad (2021), "Cybersecurity Strategy Belgium 2.0," mayo, p. 28.

[15] Centre for Cybersecurity & Homeland Security (2016), "The Private Sector and Active Defense against Cyber Threats", George Washington University, octubre, p. xi.

[16] Robert Dewar (2017), "Active Cyber Defence", CSS, ETH Zürich, junio.

un gobierno para neutralizar, mitigar o atribuir una operación maliciosa.[17] Para el *think tank* australiano ACDS, la CDA utiliza la inteligencia, el engaño, *threat hunting* y otras medidas legales. Complementa las medidas pasivas y proporciona inteligencia preventiva, incluye mecanismos bajo control gubernamental, pero excluye medidas ofensivas que se reservan a éste.

Entre las definiciones oficiales, y para el *National Cyber Security Centre* (NCNS) del Reino Unido, la CDA busca proteger a la mayoría de la población frente a los ciberataques más frecuentes y de mayor daño, –no de todos ni de los más sofisticados– mediante un programa en el que se prestan servicios a los sectores público y privado para detectar y corregir vulnerabilidades, gestionar incidentes o automatizar la disrupción de los ciberataques.[18] La CDA consta de medidas técnicas automatizadas diseñadas para identificar y prevenir los ciberataques, junto con la intervención humana para analizar y mitigar los mismos. Para el Centro de Ciberseguridad de Australia, la CDA consiste en aplicar proactivamente un espectro de medidas de seguridad para reforzar una red o un sistema y hacerlos más robustos, sin que equivalga a la devolución del ataque (*hacking back*).[19]

Las Fuerzas Armadas y las organizaciones de defensa colectivas cuentan con medidas ofensivas como parte de su poder cibernético, pero su desarrollo doctrinal no se aplica al contexto público-privado, aunque se dispone de algunas aproximaciones como las del Manual del Centro de Ciberdefensa de la Organización del Tratado del Atlántico Norte (OTAN) en Tallin o el Departamento de Defensa de EEUU.[20] Para éste, la defensa activa se refiere al uso de acciones ofensivas limitadas y contraataques para denegar al adversario una posición en disputa, e incluye la capacidad en tiempo real y sincronizada para descubrir, detectar, analizar y mitigar amenazas y vulnerabilidades. Además, implica acciones proactivas, anticipatorias y reaccionarias contra el adversario. Una de sus claves es la capacidad de consumir inteligencia para no tener que esperar a que ocurra un ataque para actuar. Incluye interceptar, interrumpir o disuadir un ataque o preparación de éste, pudiendo realizarse de forma preventiva o en defensa propia para limitar o eliminar la capacidad operativa del adversario.

2. La implantación de las medidas CDA

La validación de todos estos conceptos ha sido difícil por la naturaleza clasificada de las acciones ofensivas (no se hacen públicos ni fracasos ni éxitos) y por la dificultad de medir su impacto (los ataques se siguen produciendo, pero también se evitan). La aceptación de las medidas CDA no ha estado exenta de debate por sus implicaciones jurídicas, éticas y prácticas –tal y como se detalla posteriormente–, pero progresivamente se ha ido abriendo su necesidad. Admitida la necesidad de contar con medidas CDA, el debate se traslada a qué medidas de todas las posibles utilizan los

[17] Sven Herpig (2021), "Active Cyber Defence operations. Assessment and Safeguards", Stiftung Neue Verantwortung, noviembre, p. 7.

[18] NCSC (2024), "Active Cyber Defence 2.0", 2/VIII/2024, p. 78.

[19] La Estrategia de Ciberseguridad de Australia de 2020 no usa el término CDA sino prevenir activamente ciberataques y defender activamente Australia o las infraestructura críticas. Gobierno de Australia (2023), "Australian Cyber Security Strategy 2023-2030".

[20] Congressional Research Service (2022), "Cyberspace Operations", 2/XII/2022.

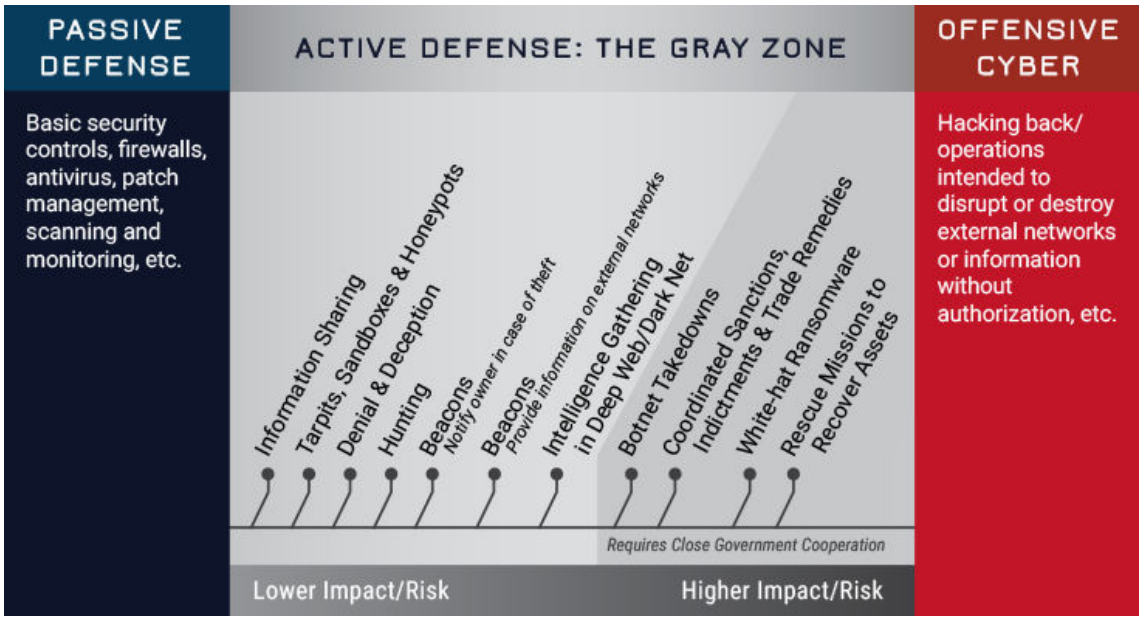
distintos actores, desde las de detección y neutralización a las de devolución de ataques (*hacking back*) o las de ciberguerra.

Aplicar las medidas CDA conlleva un riesgo, tanto si se rechaza usarlas como si se emplean, porque ambas opciones presentan contraindicaciones. Y como el resto de las gestiones de ciberseguridad y ciberdefensa, se abordan con un enfoque de riesgo, evaluando los mismos y adoptando las medidas de diligencia adecuadas. La utilización de CDA por actores públicos y privados presenta dudas jurídicas, éticas y prácticas. Lo primero, porque no existe regulación internacional ni nacional que delimite legalmente su empleo, lo que genera inseguridad sobre los márgenes de actuación. Lo segundo, porque el derecho a la propia defensa difícilmente justifica replicar la ilegalidad de los ciberataques, y lo tercero porque, a falta de información sobre efectos concretos, resulta difícil valorar su eficacia. Como es lógico, cada sociedad tiene su propio apetito de riesgo en función de la percepción social, las experiencias directas y la presión internacional para modular el empleo de la CDA, pero los casos presentados muestran que esa cultura puede evolucionar de acuerdo con las circunstancias y el liderazgo político.

La indefinición es, también, el resultado de aplicar normas y conceptos derivados del derecho internacional, de los conflictos y de las doctrinas estratégicas a un nuevo dominio de enfrentamiento como el de las denominadas guerras híbridas, donde no encajan con facilidad. Las medidas CDA se desenvuelven en la ambigüedad de la zona gris de la Figura 3, entre las medidas pasivas de protección y las claramente ofensivas, por lo que su empleo precisa justificar su legalidad y legitimidad, así como una valoración previa de los elementos jurídicos, éticos y prácticos, algo que no ocurre con las otras dos zonas.

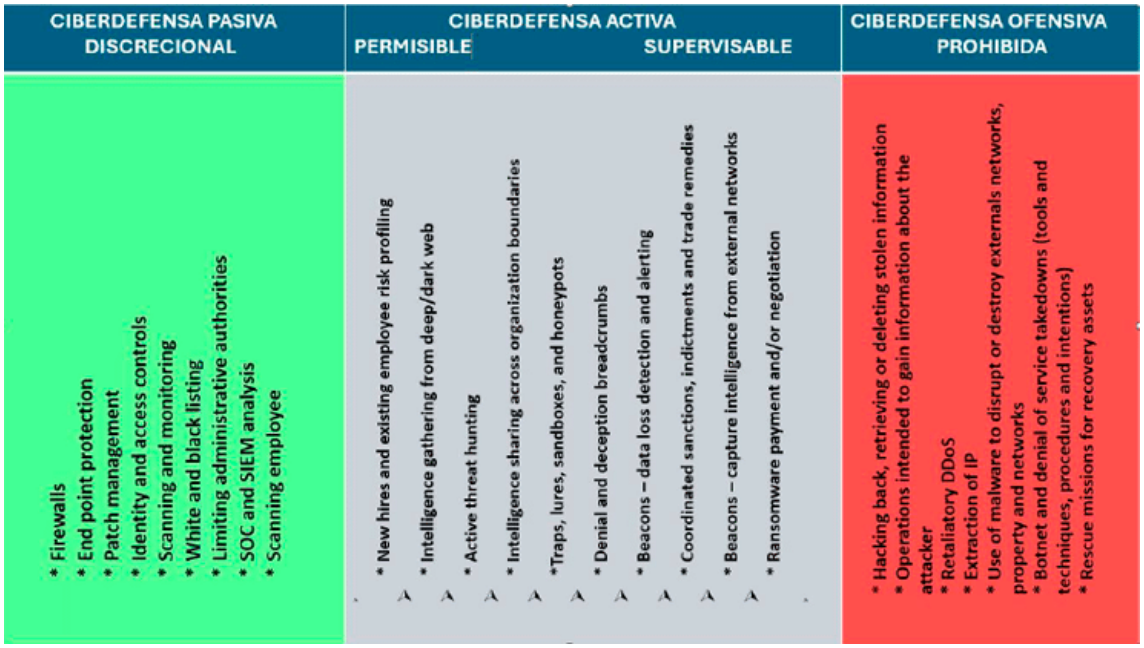
La Figura 3 muestra medidas de defensa activa en la zona gris distribuidas en función del impacto y el riesgo. Cada actor debe clasificar esas medidas de acuerdo con su valoración de riesgos (pasiva, activa y ofensiva) y trasladarla a una regulación en la que se establezca qué es discrecional, permisible, supervisable o prohibido según sugiere la Figura 3 bis.

Figura 3. El continuo entre medidas defensivas y ofensivas



Fuente: Centre for Cyber and Homeland Security.

Figura 3bis. El continuo entre medidas defensivas y ofensivas



Fuente: elaboración propia.

La observación de algunos principios como la subsidiariedad (ninguna otra opción), la proporcionalidad, la inmediatez (no la represalia), los efectos no deseados (daños a terceros) o la certidumbre (atribución) entre otros, complica el recurso a estas medidas por los sectores público y privado.[21] La mayoría de las medidas ofensivas de la zona

[21] Salome Stevens (2020), "A Framework for Ethical Cyber-Defence for Companies", en *The Ethics of Cybersecurity*", International Library of Ethics, Law and Technology, vol. 21, pp. 319- 327.

gris, tanto las dirigidas contra las redes criminales como las que combaten amenazas persistentes actúan generalmente fuera del espacio nacional, en todo o en parte, y sin autorización. Cada operación es un caso peculiar y resulta difícil elaborar marcos normativos en los que encajen todos los supuestos.

Por eso, el riesgo de empleo disminuye si los gobiernos elaboran marcos regulatorios que permitan a las organizaciones aplicar medidas de defensa activa de manera legal y ética. Los marcos regulatorios se apoyan en las estrategias de seguridad nacional, las de defensa, las de política exterior, las de seguridad y ciberseguridad, donde se admite y justifica su existencia –como principio general– y su desarrollo se realiza mediante guías políticas que orienten a sus responsables sobre su empleo. En los mismos marcos se establecen la jerarquía, requisitos y funcionamiento del ecosistema (*hub*) público-privado de CDA.

Dentro del enfoque de riesgo aplicable a las medidas CDA, es exigible que las organizaciones que las aplican dispongan de un nivel adecuado de madurez para evitar efectos no deseados. Por ejemplo, el Departamento de Defensa de EEUU (DoD) desarrolla un programa de certificación (*Cybersecurity Maturity Model Certification*) que faculta, a las industrias privadas que participan, el cumplimiento con los estándares exigidos para cooperar con el sector de la defensa.[22] La colaboración público-privada en materia CDA, incluyendo la innovación y el desarrollo de instrumentos, los ejercicios de adiestramiento, la compartición de inteligencia y otros, permite determinar los criterios de madurez para emplear las herramientas disponibles.

Existen pocas operaciones sobre las que se disponga de información en fuentes abiertas tales como las llevadas a cabo en 2021 por la Oficina Federal de Investigación estadounidense (FBI) (operación Hafnium) o por la Oficina Federal de Investigación Criminal alemana (BKA) (operación Emotet).[23] Cada operación se debe valorar caso por caso, pero existen algunos elementos de partida a tener siempre en consideración, tales como:

- Marco regulatorio, nacional o internacional, aplicable;
- Marco declaratorio (comunicación estratégica, trasparencia y auditoría);
- Objetivo (mitigar, neutralizar y atribuir el impacto);
- Efecto (estado final pretendido de la operación en cuanto a intrusión, alcance, objetivo);
- Actores (gobierno, coaliciones);
- Cronografía (atribución, tiempo);
- Operaciones (escalada, desescalada, automatización, frecuencia, costes de acción e inacción, daños colaterales).

[22] Departamento de Defensa, “Cyber Security Strategy 2018”, p. 8.

[23] El FBI realizó la operación Hafnium en 2021 para eliminar los *shells web* de los sistemas informáticos derivados de la explotación de *ProxyLogon* por parte del grupo Hafnium, vulnerabilidades de tipo *zero-day* que afectaban a Microsoft Exchange Server. La BKA llevó a cabo la operación Emotet para neutralizar el *botnet* del mismo nombre que facilitaba la descarga y ejecución de *malware*.

De los elementos anteriores, hay que resaltar la importancia de reforzar la legitimidad de las medidas CDA mediante iniciativas que refuercen su comunicación estratégica, en particular:

- Declaración de aplicabilidad o, en su defecto, de los casos de exclusión;
- Regulación nacional según el interés público-privado a proteger;
- Contribución activa a la regulación y prácticas internacionales de países aliados;
- Acceder a las capacidades y ejercitarse en las operaciones.

El reconocimiento de la disposición a emplear medidas CDA por los gobiernos, sea individual o colectivamente, establece nuevas prácticas y marcos de regulación que consolidan su aceptación en la política internacional. Progresivamente se definen comportamientos responsables, se incrementan las medidas de precaución para disminuir los riesgos y se acuerdan protocolos colectivos de actuación. Los gobiernos deben desarrollar guías de actuación explicando cómo esperan demostrar la diligencia debida en una gestión que es, por naturaleza, de riesgo.

A falta de directrices sobre la diligencia debida en el uso de CDA, Sven Harpig[24] recomienda las siguientes:

1. Se responde, pero no se venga: no se emplea en operaciones de represalia, que no servirían para la defensa de las víctimas ni se consideraría una respuesta.
2. Priorizar los espacios de aplicación: no se despliega en cualquier jurisdicción, únicamente en la nacional o, en su caso, junto a países aliados (en la zona gris de actuación, donde hay menos limitaciones).
3. No basta hacerlo, hay que explicarlo**:** los marcos de aplicación deben incluir la trasparencia y la evaluación de efectos en la comunicación estratégica.
4. Establecer un discurso internacional: los gobiernos deben ser conscientes de su papel en la configuración del derecho internacional regulando el uso responsable de la CDA.
5. Seleccionar los ejecutores de la CDA: equipos que cuenten con excelencia técnica, experiencia operativa y la voluntad de someterse a marcos de actuación estrictos bajo el mando de una autoridad central.
6. Conocer al adversario: un profundo nivel de comprensión técnica del entorno operativo del adversario es crucial para operaciones CDA.
7. Entrenar sus capacidades**:** el diseño y la prueba de capacidades debe ser minucioso para garantizar la eficiencia, eficacia y proporcionalidad de las medidas CDA.
8. Ser selectivo y preciso en el objetivo: en todo espacio operativo, las medidas deben ser lo más limitadas posible, evitando la afectación de terceros, especialmente cadenas de suministro e infraestructuras críticas.
9. De último recurso**:** los gobiernos deben ser conscientes de que toda operación activa de ciberdefensa intrusiva es probablemente una actividad única que requiere

[24] Sven Harpig (2023), “Active Cyber Defence. Toward Operational Norms”, Stiftung Neue Verantwortung, noviembre, pp. 5-9.

muchos recursos pero que, sin embargo, no mejora a largo plazo el nivel general de ciberseguridad o resiliencia del país.

3. Catálogo de medidas

Las medidas de defensa pasiva son acciones permitidas sin excepción alguna e imprescindibles para ofrecer niveles mínimos de ciberseguridad y ciberdefensa en la red propia. Son de impacto, riesgo y efecto menor en relación con medidas de ciberdefensa activa. Entre los ejemplos de acciones de defensa pasiva, básicas y habituales pueden señalarse:

- Emplear cortafuegos y *software* de detección de *malware*, intrusos y similares; parcheado del *software*; protección de terminales (*end points*) y de la información (cifrado); mantener listas blancas y negras de direcciones IP, de webs, usuarios, etc.; escanear y monitorizar los puertos y las comunicaciones de los empleados.
- Compartir indicadores de compromiso y otros datos con proveedores de seguridad para ajustar o reconfigurar sus productos; disponer de centros SOC para analizar la red corporativa y el control de identidad, el acceso de los usuarios y administradores a la misma (SIEM) o la limitación de privilegios de administrador; y la monitorización de la actividad de los empleados en la red corporativa.

La ciberdefensa activa es una extensión de la ciberdefensa pasiva. Sus operaciones puedan ser en ocasiones intrusivas y formar parte de operaciones en el ciberespacio de mayor alcance. Por eso cada regulación establece qué medidas se pueden llevar a cabo sin supervisión y cuáles la precisan (todas las medidas CDA se deben autorizar/catalogar mediante regulación). Entre los ejemplos más notorios (Figuras 3 y 3bis) figuran:

- Interacciones técnicas para atraer y analizar el comportamiento de los atacantes (*honeypots*, *tarpits* y *sandboxing*) desde las de menor riesgo como el intercambio de información y el uso de *honeypots* a las que requieren una coordinación estrecha con el gobierno como la desarticulación de *botnets* y el uso de *ransomware* de sombrero blanco.
- Recolección de inteligencia: en la *deep web* y *dark net*, así como el uso de balizas para rastrear el movimiento de archivos robados y otros indicadores de compromisos.

A continuación, se citan ejemplos de interacciones técnicas y de inteligencia que se consideran incluidas en la categoría de ciberdefensa activa (la enumeración no es exhaustiva y se presenta en orden creciente de impacto y riesgo):

- Compartición de ciberinteligencia con otras organizaciones.
- Perfilado de seguridad de los empleados y de potenciales incorporaciones.
- Emplazar señuelos en la red (*honeypots*) atraer a los atacantes con datos o información inocua y analizar su comportamiento.

- Cambio regular y cuasi-aleatorio de direcciones IP (*address hopping*) durante la transmisión de datos para dificultar el seguimiento por parte de los atacantes.
- Insertar virus benignos de tipo gusano (*white worms*) en la red protegida para buscar y destruir intrusiones maliciosas dentro de una red.
- Crear una ruta de entrada o sumidero (*sinkhole*) para tomar el control de la infraestructura de mando y control de los atacantes utilizada en campañas cibernéticas maliciosas (por ejemplo, de *botnets*); y desinstalar o neutralizar *malware* instalado en los sistemas de las víctimas y/o implementar parches.
- Emplear *cookies* del navegador (*honeytokens*) que permitan conocer la ubicación real y navegación del atacante siempre que éste no borre la caché del navegador, evitando el bloqueo de los puertos de entrada del atacante.
- Localizar usuarios que filtran o venden información no autorizada cuando ejecutan un archivo mediante un marcador o rastreador que avisa al servidor de la víctima (*canarytoken*).
- Explotar vulnerabilidades y emplear *malware* para comprometer la infraestructura de atacantes, monitorizar sus actividades, atribuir técnicamente una campaña cibernética maliciosa o interrumpir sus actividades.
- Insertar balizas (*web beacons*) para la detección y alerta de extracción de información, los movimientos del intruso en la red y la captura de inteligencia de redes externas. Contienen un enlace a internet prácticamente indetectable por el usuario y en cuanto un atacante los acciona, la organización que lo creó recibe una notificación con detalles del sistema informático del atacante y su ubicación en internet.
- Establecer direcciones de correo electrónico falsas ubicadas en su servidor de correo de la empresa o en un servidor web público para atraer los mensajes de *phishing* o *spam* de los atacantes, detectar campañas de *phishing* hacia la empresa e información sobre los métodos utilizados contra cada organización.
- Insertar información falsa en las bases de datos de una organización para que el atacante sustraiga y publique dicha información, lo que proporcionará información a la organización sobre el acceso a los sistemas corporativos y redes, así como la explotación de vulnerabilidades.
- Implantar falsos ejecutables (.exe) de apariencia legítima que permitan obtener información del atacante que los ejecute, como su dirección IP, o incluso cause daños a su sistema al revelar detalles.
- Establecer claves de Amazon Web Services falsas en ubicaciones como escritorios, repositorios de GitHub y archivos de texto. Estas claves digitales con mecanismos de registro integrados permiten controlar la infraestructura de una organización u obtener acceso a las redes corporativas. Una vez que el atacante las utiliza para obtener acceso ilícito al sistema, la organización puede usarlas como *honeytokens* para analizar, monitorear y registrar las acciones del delincuente.
- Solicitar a los proveedores de servicios de acceso a Internet (ISP) el bloqueo o redirección de tráfico malicioso, mantener en un *sandbox* los sistemas de cliente comprometidos ofreciendo información sobre el modo de limpiar y parchear estos sistemas o la entrega de actualizaciones y notificaciones de *software* y *hardware* más allá de los dispositivos proporcionados por el ISP.
- Obtención de inteligencia en *deep web* y/o *dark net*.

Sin embargo, determinadas interacciones técnicas de CDA necesitan la aprobación y colaboración entre los agentes privados afectados y las autoridades. Son las acciones más próximas a las medidas ofensivas y serían, por ejemplo:

- Operaciones de rescate de activos (redes, servidores, información, etc.).
- El bloqueo de *botnets*.
- La atribución de ciberataques, establecer sanciones coordinadas o la negociación con los atacantes.
- Llevar a cabo contraofensivas utilizando *ransomware* de sombrero blanco.

Las medidas ofensivas (zona roja) son acciones llevadas a cabo en activos y redes exteriores a la propia red del atacante o de terceros relacionados con éste que causan un alto impacto y son de elevado riesgo para quienes ejecutan estas medidas. Por defecto, su ejecución no está permitida a los agentes del sector privado. Ejemplos de medidas ofensivas propias del ámbito de la ciberdefensa son:

- *Hacking back* o contraataque y ocasional toma de control de los dispositivos y/o de la red del atacante.
- Operaciones en los activos del atacante o de terceros destinadas a interrumpir o destruir mediante *malware* redes, datos e información, recuperar y borrar la información robada y obtener información del atacante.
- Disrupción de la red del atacante mediante *botnets* o ataques por denegación de servicio (DDoS).

4. Casos-estudio de Ciberdefensa Activa

Progresivamente, aumenta el número de países que admiten la disponibilidad o el desarrollo de medidas CDA y de ecosistemas (*hub*) de desarrollo.

El Departamento de Defensa de EEUU acuñó el término de ciberdefensa activa por primera vez en 2011 y ha seguido desarrollando sus capacidades defensivas y ofensivas para adaptarse a su papel de potencia mundial en el exterior, –que "compita, disuada y gane" en el dominio del ciberespacio– mientras que el Departamento de Seguridad Interior ha desarrollado medidas de defensa activas y pasivas en el ámbito de la ciberseguridad. Los sucesivos documentos estratégicos han apoyado el empleo de capacidades y conceptos ofensivos en todo el espectro del conflicto. El sector privado de EEUU se ha distinguido por reivindicar la implantación y regulación de las medidas CDA, no sólo para recibir protección gubernamental, sino también para participar en la política de disuasión cibernética. Ha solicitado la adaptación de leyes existentes como la del *Computer Fraud and Abuse Act* para permitir ciertas formas de defensa activa dentro de los límites legales.[25] En contrapartida, los gobiernos estadounidenses tratan de consolidar estructuras de integración de las capacidades CDA del sector privado con las capacidades regulatorias de las agencias federales, al tiempo que el Mando de Ciberdefensa (USCYBERCOM) y la Agencia de Ciberdefensa (CISA) incrementan los

[25] David A. Simon (2017), "Raising the Consequences of Hacking American Companies. Why the United States Needs an Explicit Cyber Deterrence Policy for the Private Sector", CSIS, octubre.

partenariados con actores públicos y privados para mejorar las capacidades de ciberdefensa.[26]

Francia se ha manifestado abiertamente a favor de convertirse en otra potencia cibernética con capacidad defensivas y ofensivas y ha expresado esa condición en todos sus documentos estratégicos desde el Libro Blanco de Defensa de 2008[27] a la Revisión Estratégica de la Defensa de 2018.[28] El primero abogaba por una transición desde una estrategia de defensa pasiva defensiva a otra de defensa activa en profundidad, combinando sistemas de vigilancia, respuesta rápida y acción ofensiva, lo que implicaba un cambio de mentalidades. Los gobiernos han atribuido la conducción de operaciones ofensivas a las fuerzas armadas y hecho públicos los principios de las doctrinas militares defensivas y ofensivas. La creación de la *Agence Nationale de la Sécurité des Systemes d'Information* (ANSSI), un organo interministerial dentro de la Secretaría General de Seguridad y Defensa Nacional (SGDSN), permite mantener el control a lo largo de la escalada de respuesta. El sector privado colabora con la ANSSI y el Ministerio de Defensa mediante acuerdos público-privados para compartir recursos, inteligencia, ejercicios, investigación y desarrollo y otras actuaciones de ciberdefensa activa. Francia está en contra de la devolución de ataques y promueve su regulación internacional para prevenir escaladas.

El Reino Unido incluyó su capacidad de defensa activa en la Estrategia Nacional de Ciberseguridad 2016-2021 para la protección de activos civiles frente a ciberataques que no conllevaran riesgo de una escalada militar.[29] La Estrategia 2022-2030 prorrogó la prestación de las capacidades CDA que el *National Cyber Security Center* (NCSC) proporciona a los sectores públicos, preferentemente, pero también al privado dentro de un programa que acaba de revisar.[30] En las estrategias declara su voluntad de cubrir todo el espectro de operaciones incluidas las ofensivas (*advanced protections*) contra las amenazas más sofisticadas. Cuenta para ello con una organización, la *National Cyber Force*, y un marco legal para hacerlo (*Intelligence Services Act* 1994, ISA), *Investigatory Powers Act* 2016 (IPA) y *Regulation of Investigatory Powers Act* 2000 (RIPA).[31]

El enfoque británico del programa CDA busca la colaboración público-privada en un régimen de trasparencia, confianza e incentivos para automatizar la respuesta a escala nacional frente a los ataques comunes y permitir a los defensores centrarse en los ataques más sofisticados. El Reino Unido ha declarado su interés por contar con capacidades defensivas y ofensivas desde 2007. Dispone del NCSC para ejecutar su programa de CDA desde 2016 y coordinar la respuesta público-privado a los ciberataques. Desarrolla acciones y presta servicios de inteligencia, orientación técnica,

[26] The White House (2023), "National Cybersecurity Strategy", marzo, p. 15. Ver los programos Joint Cyber Defense Collaborative (JCDC) Resources de CISA y Under Advisement (UNAD) de CYBERCOM.

[27] Presidente del Gobierno (2008), "The French White Paper on Defence and National Security", p. 50.

[28] Secretaría General de la Defensa Nacional (2018), "Revue stratégique de cyberdéfense", febrero.

[29] Tim Stevens *et al.* (2019), "UK Active Cyberdefence", The Policy Institute, King's Collegue, enero.

[30] NCSC (2024), "Active Cyber Defence 2.0", 2/VIII/2024, p. 45. El NCSC tiene un Active Cyber Defence hub que proporciona una serie de servicios.

[31] National Cyber Force (2023), "Responsible Cyber Power in Practice", marzo.

innovación y ejercicios de ciberdefensa tanto para el sector público, principalmente, como para el sector privado.[32]

Alemania inició su apertura a la CDA a partir del ciberataque al Parlamento alemán de 2015. Una apertura condicionada por las limitaciones legales, doctrinales e ideológicas a las acciones ofensivas, por lo que cada nueva medida precisa adaptar previamente sus marcos de anclaje.[33] En su Estrategia de Ciberseguridad de 2016 admitió la posibilidad de llevar a cabo operaciones en respuesta a ciberataques graves que no pueden ser gestionados con medidas preventivas clásicas en el tiempo requerido, quedando a cargo del gobierno federal la evaluación de las condiciones legales y técnicas para implementar tales operaciones. Las Fuerzas Armadas alemanas disponen de capacidades ofensivas de ciberdefensa que se enmarcan en su mandato constitucional y el derecho internacional, unas capacidades que se han ido desarrollando dentro de la defensa y la seguridad colectiva de la OTAN y de la UE y de la protección de las infraestructuras críticas, para las que la Estrategia de Ciberseguridad de 2021 prevé medidas proactivas y no sólo reactivas. Sin embargo, las medidas CDA en general y las de ataques de represalia en particular han encontrado dificultades para progresar.[34] De hecho, y en su primera Estrategia de Seguridad Nacional de 2023, el gobierno federal descartó la idea de tomar medidas de contraataque (*hacking back*) como medio de ciberdefensa y se comprometió a examinar qué capacidades y competencias jurídicas requiere para protegerse de un ciberataque en curso o inminente.[35]

A estos países, se añaden otros que han ido incluyendo la CDA entre sus capacidades de respuesta. El Plan de Acción de Ciberseguridad de Italia de 2017 admitió la necesidad de adoptar tácticas de defensa activa para complementar las medidas pasivas y mejorar la diligencia debida.[36] La peculiariedad de Israel en cuanto a medidas CDA es la defensa del sector privado en las estrategias gubernamentales, tanto a través del *National Cyber Directorate* como mediante servicios privados de ciberseguridad.[37] El desarrollo de esos servicios y una mayor proclividad a posiciones ofensivas en la cultura estratégica israelí han proporcionado resiliencia y una capacidad de defensa activa al ecosistema civil-militar israelí que no tienen otros países. A lo anterior, se une una doctrina de empleo entre guerras (*campaign between campaigns*, CBC) dentro de la zona gris y sin escalar a un conflicto armado abierto que le permite poner a punto sus capacidades, doctrinas y procedimientos.[38] Su concepto de ciberdefensa nacional permite realizar medidas de ciberdefensa activa y acciones ofensivas a sus órganos de

[32] Active Cyber Defence Program, p. 125.

[33] Sven Herpig, Robert Morgus y Amit Sheniak (2020), "What is Active Cyber Defense", Konrad Adenauer Stiftung, marzo.

[34] Sven Herpig (2021), "Active Cyber Defence operations. Assessment and Safeguards", Stiftung Neue Verantwortung, noviembre, pp. 15-29; Annegret Bendiek y Jakob Bund (2023), "Shifting Paradigms in Europe's Approach to Cyber Defence", *SWP Comment* 4, 8/IX/2023.

[35] Gobierno Federal, "Estrategia de Seguridad Nacional", p. 62.

[36] Italian Cyber Security Action Plan, p. 11.

[37] Sven Herpig, Robert Morgus y Amit Sheniak (2020), "What is Active Cyber Defense", Konrad Adenauer Stiftung, marzo 2020, p. 6.

[38] David Siman-Tov (2022), "Cyber Attacks Are Escalating Israel's 'Campaign Between Wars', The National Interest, 1/VII/2022.

seguridad nacional y agencias de seguridad contra actores estatales y no estatales, en una función netamente intergubernamental llevada a cabo de forma autónoma o con terceros.

A diferencia de los casos estudio anteriores, la Unión Europea (UE) ha evolucionado desde la ciberseguridad, con sus competencias de seguridad interior y mercado digital único, hacia la ciberdefensa, donde no dispone de más capacidades que las que le presten sus Estados miembros. El concepto de CDA de la UE ha evolucionado en paralelo a la amenaza, sin que todavía cuente con una definición ni un marco regulatorio adecuado.[39] La UE se ha limitado a apoyar las iniciativas de los Estados miembros y la Estrategia de Ciberseguridad de 2020 reconoció la necesidad de "disponer de capacidad operativa para prevenir, disuadir y responder".[40] En 2022, la UE adoptó una política de ciberdefensa en la que solicitaba a los Estados miembros reforzar sus capacidades en todo el espectro de la ciberdefensa, incluyendo las capacidades de defensa activa.[41] La UE apoya el desarrollo de capacidades de defensa, incluidas medidas defensivas proactivas para proteger, detectar, defender y disuadir ciberataques pero éstas no se incluyen en el inventario de sus respuestas diplomáticas (*diplomacy toolkit*).

Entre los últimos apoyos de la UE al desarrollo de capacidades CDA por sus Estados miembros figura la Directiva sobre la seguridad y redes de la información (Directiva NIS2). Aunque excluye las medidas ofensivas, recomienda a los Estados que adopten "políticas de fomento de la ciberprotección activa" a diferencia de las respuestas reactivas. En la misma línea, el informe para la Comisión Europea de Sauli Niinistö recomienda "hacer algo más para disuadir creíblemente a los actores maliciosos", incluyendo la disuasión por denegación y por castigo".

Finalmente, y en relación con el desarrollo de *hubs* CDA, hay que incluir la creación por la OTAN de un Centro Integrado de Ciberdefensa en Mons (Bélgica) para integrar los centros aliados y nacionales que analizan las amenazas y desarrollan operaciones junto con las industrias especializadas que desarrollan capacidades de respuesta.

5. El estado de la ciberdefensa activa en España

En el caso de España, la valoración de la CDA es difícil porque no dispone de documentos estratégicos sobre ciberdefensa en fuentes abiertas y los que se refieren a la ciberseguridad sólo reconocen el concepto nominalmente.[42] La primera Directiva de Defensa Nacional que mencionó la ciberseguridad fue la de 2012 –la anterior de 2008 sólo mencionó el ciberespacio como un nuevo ámbito de operaciones– para señalar que

[39] Annegret Bendiek y Jakob Bund (2023), "Shifting Paradigms in Europe's Approach to Cyber Defence", *SWP Comment* 4, 8/IX/2023.

[40] Jaap de Hoop Scheffer (2018), "Strengthening the Eu's Cyber Defence Capabilities", CEPS Task Force, noviembre, pp. 41-45.

[41] Alto Representante, JOIN (2022) 49 final sobre ciberdefensa, (10/XI/2022), p. 1.

[42] La investigación no ha podido acceder a la visión del JEMAD de la Ciberdefensa Militar ni al concepto de Ciberdefensa Militar, ambos de 2011, al Plan de Acción para la Obtención de la Capacidad de Ciberdefensa de 2012, a la Estrategia Conjunta de Ciberdefensa de 2012 y al Documento Marco de la Ciberdefensa Nacional de 2014 por no estar disponibles en fuentes abiertas. Esto impide analizar las directrices del Mando Conjunto de Ciberdefensa implantado en 2013.

la participación militar se llevaría a cabo dentro del marco establecido por las estrategias de seguridad nacional, tal y como han venido reiterando las directivas posteriores. Las estrategias de seguridad nacional de 2017 y 2021 no mencionan el término ciberdefensa que sí se incluyó en la Estrategia de 2013, por lo que ésta se considera parte de la ciberseguridad e integrada en el sistema de seguridad nacional. Una consideración que compartía el Concepto Operativo de las Fuerzas Armadas de 2017, así como el Marco Legal para el Empleo de las Fuerzas Armadas de 2021 en las que la ciberdefensa era la parte de ciberseguridad bajo responsabilidad militar que incluían los incidentes dentro de las Fuerzas Armadas y cualquier "respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional". Un primer reconocimiento de la defensa activa corresponde al Instituto Nacional de Ciberseguridad (INCIBE) que advirtió en 2018 sobre el interés de la inteligencia y la defensa activa para el sector industrial y su novedad respecto a las arquitecturas y defensa pasiva tradicionales, tal y como muestra la Figura 4. La defensa activa no incluía el *hacking back* y se limitaba a medidas de monitorización, detección, análisis, reacción y consumo de inteligencia.

Figura 4. La arquitectura de ciberseguridad ampliada

Fuente: INCIBE.[43]

En 2019, la Estrategia de Ciberseguridad Nacional amplió el concepto de ciberdefensa por el lado civil y reconoció que "La defensa de ciudadanos, autónomos y empresas debe ir más allá de las medidas de autoprotección que ellos puedan tomar, por lo que es conveniente implantar medidas para su ciberdefensa activa",[44] medidas que la Estrategia iba a establecer en los sectores público y privado. En 2020, la Directiva de Política de Defensa propuso potenciar la colaboración civil y militar para hacer frente a posibles amenazas en el ciberespacio, el espacio exterior y a las estrategias híbridas, tratando de alcanzar una mejor comprensión del entorno y de la zona gris por debajo de otros umbrales de respuesta.[45] Dentro del marco cívico-militar de cooperación, la Estrategia de Seguridad Nacional de 2021 propuso entre sus prioridades la creación de un sistema de observación y medición de la situación de la ciberseguridad nacional y la puesta en marcha de una plataforma nacional de notificación y seguimiento de ciberincidentes que permita medir el intercambio de información entre organismos públicos y privados en tiempo real, propuestas que siguen pendientes de ejecución.

[43] INCIBE (2018), "Defensa activa e inteligencia: de la teoría a la práctica", 2/VIII/2018.

[44] Dpto. Seguridad Nacional (2019), "Estrategia de Ciberseguridad Nacional, p.37.

[45] Directiva de Política de Defensa, agosto 2020, apdo. 6.

A falta de una regulación conceptual de la ciberdefensa activa, ésta se desarrolla de forma dispersa. El Centro Criptológico Nacional (CCN-CERT) emplea abiertamente el término para referirse a las medidas que desarrolla para responder ante las agresiones. Son medidas como las de la Figura 5, que tienen naturaleza pasiva y se añaden a las que se proporcionan para protección (Esquema Nacional de Seguridad) y vigilancia (Red de Centros de Operaciones de Seguridad, SOC) a las administraciones públicas, por lo que no casarían con el concepto de CDA descrito en este texto.

Figura 5. Medidas CDA del CCN-CERT

Fuente: Jornadas CCN-CERT.

En todo caso, las grandes empresas llevan a cabo medidas similares orientadas a la anticipación, detección temprana y contextualización de incidentes como:

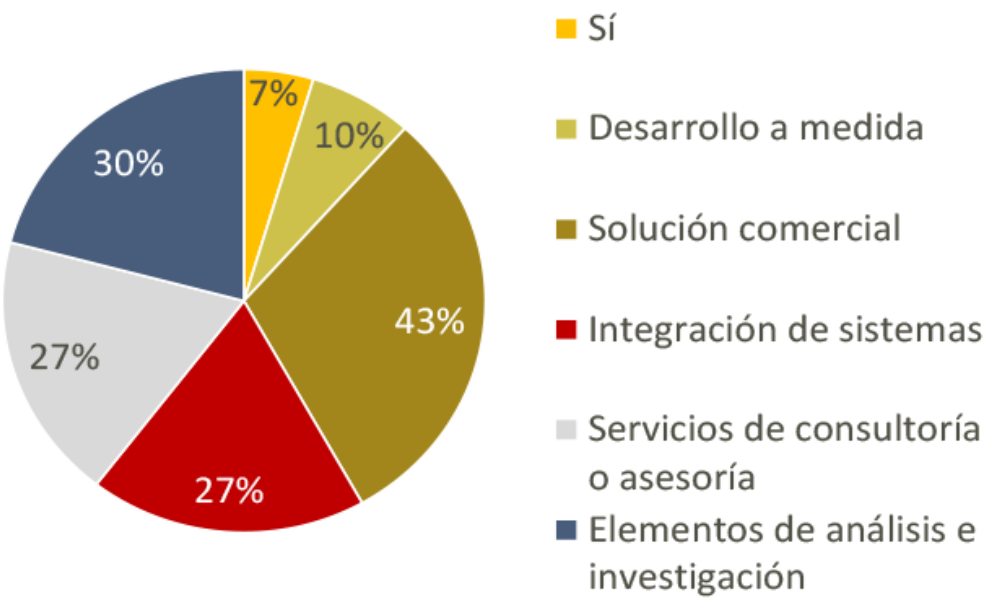
- recopilación de información y elaboración de análisis de fuentes OSINT;
- identificación de grupos de amenazas específicos y sus técnicas, tácticas y procedimientos;
- *hacking* ético para probar, con mentalidad de atacante, el grado de protección de sus sistemas (a ser posible en relación con la anterior);
- *hunting* (en combinación con las anteriores);
- *honeypots*: con la incorporación de sistemas, documentos, informaciones, cuentas y correos que sirvan de alarma y faciliten inteligencia sobre los atacantes;
- *sinkholes* y solicitudes formales de supresión de dominios maliciosos o webs implicadas en incidentes.

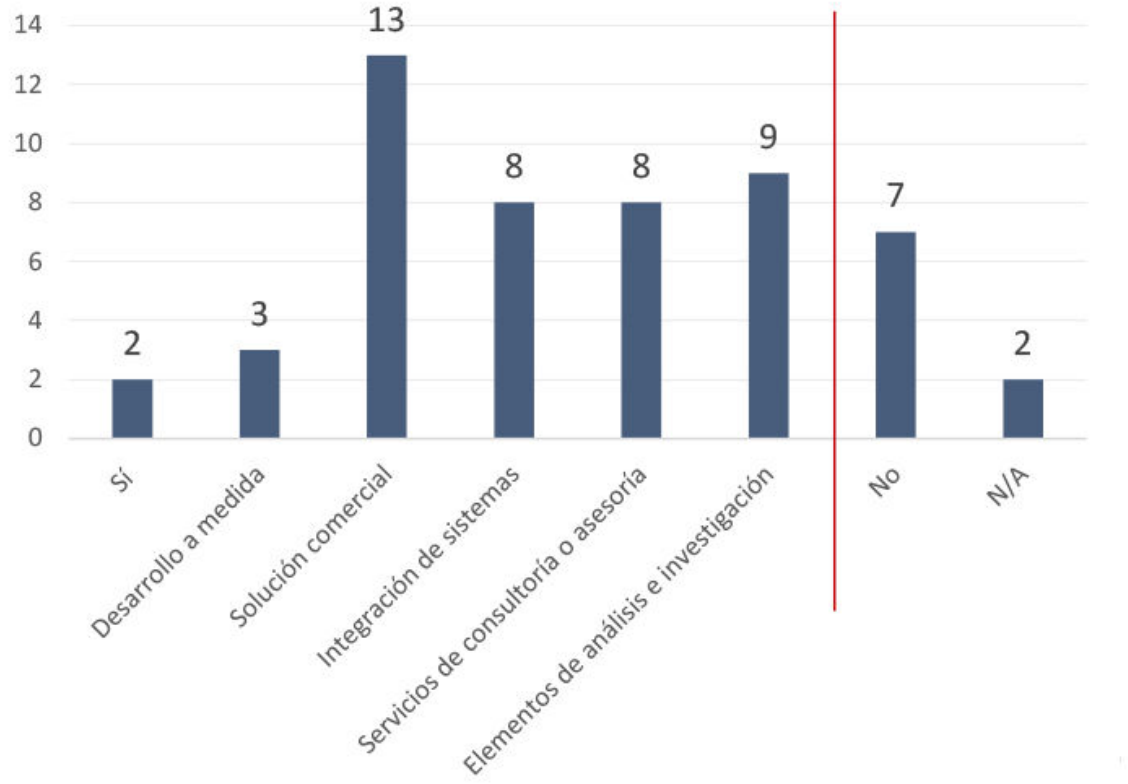
Son medidas que se pueden encajar en la zona gris de la CDA y que se practican sin soporte conceptual y normativo. Por el contrario, no explotan vulnerabilidades ni denegaciones de servicios contra sistemas de terceros (sean de los atacantes o de los colonizados por ellos) ni emplean *malware* para acceder, explorar y controlar esos activos. Tampoco la realizan o, al menos, se reservan el derecho de hacerlo por ellos organizaciones gubernamentales como el Centro Criptológico Nacional, el INCIBE y el Mando Conjunto del Ciberespacio.

Una vez admitido el derecho a la ciberdefensa activa y reconocido el empleo de algunas de sus medidas, queda por saber de qué espectro de capacidades CDA se dispone. Como se ha visto, la cooperación público-privada coadyuba al desarrollo de tecnologías e industrias nacionales que proporcionen autonomía estratégica en materia CDA, aunque España no dispone de un *hub* similar a los mencionados. Para una aproximación a las capacidades se puede recurrir a los análisis del Foro Nacional de Ciberseguridad sobre la cooperación público-privada en materia industrial. Estos consideran medidas de defensa activa las que contrarrestan riesgos detectados o ciberataques que se están ejecutando o se van a ejecutar y permiten aprender, prevenir o mitigar métodos de agresión.

El estudio elaborado con base en un cuestionario con las industrias del sector muestra la limitada oferta industrial y la falta de un programa de investigación específico. La Figura 6 muestra las funciones aplicables a las medidas CDA a las que se dedican las industrias del sector. Casi un tercio no desarrolla ninguna función aplicable, sólo dos empresas reconocen desarrollar medidas a demanda (7%) y la mitad de las empresas que disponen de capacidades proceden de compra comercial (43%).

Figura 6. Funciones aplicables a las medidas CDA a las que se dedican las industrias del sector





Fuente: Foro Nacional de Ciberseguridad, 2023.

La encuesta revela que gran parte del sector desconoce la diferencia entre las medidas activas y las pasivas. En el aspecto positivo, algunas empresas desarrollan soluciones centradas en la decepción, la disrupción o la disuasión, así como a recabar inteligencia sobre tácticas, técnicas y procedimientos (TTP) de agresión. Entre las que aplican soluciones comerciales se dedican a la monitorización, recopilación, detección, aislamiento y disuasión. [46] Como resultado, el Informe recomienda la amplia potenciación de la industria nacional para los sistemas de defensa, en general, y para los de defensa activa en particular.

Conclusiones

Recomendaciones para la implantación de la Ciberdefensa Activa en España

España tiene un problema de ciberseguridad porque las estrategias, políticas e inversiones públicas no están a la altura del contexto geopolítico actual y el sector privado continúa asumiendo costes y funciones de protección que corresponden al Estado. Lo anterior revela tanto la separación estratégica de la ciberseguridad y la ciberdefensa como la necesidad de integrarlas si se desea transformar la cultura de ciberseguridad pasiva que predomina hasta ahora. Implantar la CDA facilitaría la integración en doctrinas, ejercicios, inteligencia, tecnología e industria entre los sectores

[46] Sin resultar un listado exhaustivo y a título de ejemplo, el Informe reseña algunas de estas herramientas comerciales indicadas en las respuestas: NAGIOS, Fortinet, Splunk, Tenable.IO, Crowdstrike, Cisco Umbrella, Netskope, Imperva, Proofpoint TAP, Intune/SCCM & Airwatch.

público y privado. Sin esta convergencia, el sector privado español continuaría indefenso frente a los grandes ciberdelincuentes geopolíticos y criminales porque el sector público no proporciona suficiente protección frente a ellos.

La mera admisión de la CDA, tal y como se hace en la Estrategia de Ciberseguridad Nacional, o disponer de algunas medidas, sin elaborar un concepto que delimite su función ni dotarle de un marco regulatorio o de las directrices para su desarrollo condena la CDA a la marginalidad. En un entorno de inseguridad como el descrito en el que proliferan las herramientas ofensivas en manos de los grandes grupos criminales y florece el comercio que permite su acceso comercial a agentes no especializados, renunciar a declarar públicamente la voluntad de disuadir por denegación y por castigo, va en contra de las medidas y ecosistemas de CDA en nuestro entorno e incentiva los ciberataques. Los conceptos facilitan la comunicación estratégica de la disuasión y legitiman el desarrollo de las normas legislativas y las medidas técnicas para desarrollar las capacidades adecuadas.

Los recursos públicos y privados son limitados. Sin concepto, marco normativo ni política declaratoria, no será posible desarrollar capacidades ni crear estructuras conjuntas para luchar y disuadir frente a los grandes ciberatacantes. Lo anterior desincentivará la participación del sector privado en el desarrollo de las medidas, lo que desplazará el coste de la soberanía estratégica al sector público. Como resultado, el Estado limitará su capacidad de protección y el sector privado tendrá que incrementar su esfuerzo económico en medidas de ciberseguridad pasiva, justamente lo que se quería prevenir con la adopción de la CDA.

Para evitarlo se proponen las siguientes recomendaciones:

- Elaborar un concepto de ciberdefensa activa que legitime su desarrollo (podría aprovecharse una actualización de la Estrategia de Ciberseguridad Nacional como sugiere la Directiva NIS2).
- Elaborar un marco normativo que defina sus funciones y límites, así como su modelo de gobernanza dentro del Sistema de Seguridad Nacional (podría elaborarse como Línea de Actuación de la Estrategia).
- Elaborar un Programa/Plan director de desarrollo de ciberdefensa activa que permita el desarrollo de la industria y la autonomía nacionales, preferentemente, o en colaboración con las iniciativas europeas o transatlánticas por defecto.