LA GUERRA INFORMÁTICA, PARTE 2: LA METAMORFOSIS DE LA GUERRA INFORMÁTICA, EL CONFLICTO “PERMANENTE”

(La primera parte se publicó en el Boletín del Centro Naval N.° 817 [2007], pág. 219, “La Guerra Informática”.)

Capitán de Fragata (R) Claudio López

El Capitán de Fragata (R) Claudio López, es magíster en Ciberdefensa por la Facultad de Ingeniería del Ejército y magíster en Ingeniería del Software por el ITBA y la Universidad Politécnica de Madrid. Además, posee una especialización en Criptografía y Seguridad Informática. Cuenta con una extensa trayectoria profesional en la Armada Argentina, donde se desempeñó como Jefe del Servicio de Informática de la Armada, y en el Estado Mayor Conjunto, donde ocupó cargos en la Dirección General de Comunicaciones e Informática (ex Jefatura VI).

En el ámbito académico, es director académico y docente de los cursos de posgrado en Análisis de Sistemas Automatizados para el Desarrollo de las Operaciones Militares y posgrado en Análisis de Sistemas Automatizados de Gestión para la Defensa, Producción y Logística en la Facultad de la Armada (UNDEF). Sus investigaciones actuales se centran en el uso de redes neuronales e inteligencia artificial como herramientas de asesoramiento en la ciberatribución y la defensa ante ciberataques. Es autor del libro "Inteligencia artificial en la ciberdefensa" y de numerosos artículos sobre sistemas autónomos y guerra informática.

El artículo de 2007, "La Guerra Informática", publicado en el Boletín del Centro Naval N.º 817, pág. 219, de ese mismo año, cuyo autor es el que suscribe, ofrece una visión general de lo que entonces era un ámbito emergente del conflicto. Las "operaciones informáticas" se categorizaban en ofensivas y defensivas, siendo las ofensivas aquellas vinculadas a la propagación de virus, la manipulación de datos y la guerra psicológica a través de internet, mientras que las operaciones defensivas consistían en la protección de redes y sistemas [1].

Sin embargo, el panorama de la ciberguerra ha evolucionado drásticamente desde entonces. Un análisis contemporáneo requiere un cambio de enfoque, desde los conceptos fundamentales hasta la naturaleza compleja, multidimensional y generalizada del ciberconflicto moderno.

La evolución tecnológica y el aumento exponencial del uso de internet han redefinido por completo la manera en que se libran los conflictos en el ciberespacio. Hoy, la guerra informática no solo abarca operaciones ofensivas y defensivas, sino que también incluye la manipulación de la información y la influencia sobre la opinión pública, aspectos que han adquirido una importancia estratégica sin precedentes. Así, también la competencia entre estados y actores privados se ha intensificado, generando un entorno donde la innovación constante es clave para mantenerse a la vanguardia.

Por ejemplo, hoy un administrador de sistemas de una empresa ya no se enfrenta a un archivo malicioso estático, sino que puede ser objeto de un ataque orquestado por una inteligencia artificial generativa. En cuestión de segundos, una IA puede analizar el perfil psicológico de los empleados para lanzar una campaña de *phishing* (suplantación de identidad) hiperpersonalizada, mientras un *malware* (software diseñado para dañar o infiltrarse en sistema informáticos) evolutivo altera su propia firma digital (patrón o huella técnica que permite a los antivirus reconocer un programa malicioso) en tiempo real para volverse invisible ante los antivirus convencionales. Al mismo tiempo, en las redes sociales de los ciudadanos, un *deepfake* (video o audio falso generado con IA que imita a una persona real) de un líder político, creado con una perfección inédita, comienza a viralizarse para erosionar la confianza pública y polarizar a la sociedad.

Para visualizar de manera clara este nuevo escenario con los conceptos fundamentales establecidos en 2007, la siguiente tabla detalla las diferencias clave entre la perspectiva inicial y la complejidad del escenario contemporáneo, donde la innovación constante es el único camino para mantener la iniciativa estratégica:

1 "La guerra informática" (2007). *Boletín del Centro Naval N.º 817*, p. 219. [https://cefadigital.edu.ar/bitstream/1847939/1125/1/BCN-0817.pdf]

Tabla 1: Evolución del ciberconflicto

Característica	Visión en 2007	Realidad en 2025
Actor principal	Hackers	APT (amenazas persistentes avanzadas) estatales y cibermercenarios
Objetivo	Comando y control	Infraestructura crítica y mente humana
Estrategia	Ofensiva/Defensiva discreta	Compromiso persistente (defensa avanzada)
Herramienta	Virus y manipulación de datos	IA, *deepfakes* y *malware* evolutivo

Más allá de la ofensiva y la defensa: la era del compromiso persistente

Una perspectiva más actual va más allá de la simple dicotomía entre ataque y defensa presentada en aquel artículo de 2007. El modelo estratégico actual, adoptado particularmente por las naciones líderes en capacidades cibernéticas, se basa en el compromiso persistente y en la defensa avanzada. El General Nakasone argumenta en la publicación "Una fuerza cibernética para operaciones persistentes" (2019) que, para competir eficazmente, las fuerzas cibernéticas deben buscar continuamente la iniciativa táctica y estratégica, operando de manera global y continua contra los adversarios[2]. Esta doctrina postula que, para defender eficazmente sus redes, una nación debe operar continuamente dentro de las redes del adversario. Esto representa una evolución significativa sobre las operaciones ofensivas y defensivas discretas.

El modelo estratégico actual... se basa en el compromiso persistente y en la defensa avanzada. El General Nakasone argumenta... que, para defender eficazmente sus redes, una nación debe operar continuamente dentro de las redes del adversario.

Este enfoque reconoce que el ámbito digital es un campo de batalla constante, sin una distinción clara entre tiempos de paz y tiempos de guerra. Las operaciones no se limitan a alterar o destruir datos, como se menciona en el texto de 2007, sino a recopilar inteligencia, posicionarse para futuros ataques y ejecutar campañas de influencia que no alcanzan el umbral del conflicto armado.

Este cambio implica que la defensa ya no se concibe como una barrera pasiva, sino como una actividad dinámica que requiere vigilancia constante, anticipación y respuesta proactiva. La estrategia de compromiso persistente reconoce que las amenazas evolucionan a gran velocidad y que la detección temprana de intrusiones, junto con la capacidad de contrarrestar o incluso disuadir ataques dentro de las redes enemigas, es fundamental para la seguridad nacional. En "The Pentagon's New Cyber Strategy: Defend Forward (Lawfare)" (2018), Dave Weinstein comenta la nueva estrategia cibernética del Departamento de Defensa de EE. UU. de 2018 y el concepto estratégico denominado "Defend Forward" (defender hacia adelante), que plantea la idea de interrumpir o detener actividades cibernéticas maliciosas en su origen[3].

En consecuencia, las operaciones cibernéticas se desarrollan en un ciclo continuo de operación, donde la recopilación de inteligencia, la disrupción y el análisis forense son procesos simultáneos y entrelazados. Este punto introduce la necesidad de colaboración interinstitucional y alianzas internacionales, ya que la naturaleza global del ciberespacio hace que los ataques puedan provenir de cualquier lugar y afectar a múltiples sectores. Por ello, la cooperación y el intercambio de información entre gobiernos, empresas y organismos de seguridad se han convertido en pilares esenciales de la defensa cibernética moderna.

Jeff Kosseff examina la estrategia de "Defensa avanzada" desde la perspectiva del derecho internacional. Define el concepto como un conjunto de tres componentes:

2 Paul M. Nakasone (2019). "A Cyber Force for Persistent Operations". *National Defense University Press*, p. 10. [https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf]

3 Dave Weinstein (2018). "The Pentagon's New Cyber Strategy: Defend Forward". *LAWFARE*. [https://www.lawfaremedia.org/article/pentagons-new-cyber-strategy-defend-forward?utm_source=chatgpt.com]

1. posicionamiento para degradar operaciones adversarias;
2. advertencia para recopilar información; y
3. influencia para disuadir a los adversarios[4].

Esta visión, desde el derecho internacional, subraya la importancia de equilibrar la protección con el respeto a las normas globales y pone en el centro el desafío de disuadir a los adversarios sin caer necesariamente en el enfrentamiento directo. En el contexto actual, donde las fronteras entre la guerra y la paz son cada vez más difusas, esta perspectiva invita a repensar la defensa como un ciclo continuo de inteligencia, prevención y persuasión.

La doctrina militar estadounidense ha evolucionado al respecto. El análisis de la Estrategia Cibernética del Departamento de Defensa de 2023 (*2023 DoD Cyber Strategy*) y la Estrategia Nacional de Ciberseguridad de 2023 revela un refinamiento conceptual que va más allá de la mera persistencia operativa[5].

Los nuevos actores: de la habitación del hacker a las corporaciones del espionaje. El auge de los cibermercenarios

En el artículo de 2007 se identificaban como actores relevantes a los "hackers" motivados por intereses ideológicos o políticos, que simpatizaban con una causa específica. Un ejemplo de ello se observó durante la guerra serbobosnia, donde estos individuos empleaban ataques informáticos para apoyar a sus respectivos bandos, utilizando el ciberespacio como un recurso adicional en el conflicto.

Hoy en día, las principales amenazas son mucho más sofisticadas. Los actores primordiales son las "amenazas persistentes avanzadas (APT)"[6], que suelen ser grupos patrocinados por estados con importantes recursos, talento y objetivos estratégicos. Estos grupos, como APT28 (Rusia), el Grupo Lazarus (Corea del Norte) y varias APT chinas, son responsables de importantes campañas de espionaje y sabotaje.

Además, el auge de los cibermercenarios o los grupos de *ransomware* (programa que bloquea sistemas o datos para exigir un rescate) como Clop o Akira ha comercializado la ciberguerra. Estos actores no estatales pueden ser contratados por naciones o corporaciones o actuar de forma independiente para paralizar infraestructuras críticas con fines lucrativos, lo cual hace que se difumine la línea entre la actividad estatal y la delictiva. Akira, surgido en 2023, ejemplifica cómo los actores criminales han adoptado la sofisticación de las APT, con ganancias ilícitas estimadas en 42 millones de dólares y ataques a más de 250 organizaciones críticas[7].

Estos grupos están formados por equipos de expertos, muchas veces organizados como empresas privadas que ofrecen sus servicios, ya sea para realizar ataques, desarrollar herramientas maliciosas o incluso brindar asesoría en ciberinteligencia. Estas entidades actúan ampliando el espectro de amenazas y dificultando la atribución de los ataques.

NSO Group[8], empresa israelí fundada en 2010, desarrolla Pegasus, un software espía capaz de extraer datos personales de teléfonos inteligentes. NSO afirma que vende Pegasus solo a agencias gubernamentales para combatir el crimen y el terrorismo. Sin embargo, investigaciones han revelado su uso para espiar a periodistas, abogados, disidentes y activistas, lo cual ha generado una polémica internacional por violaciones a los derechos humanos.

Black Cube[9], otra agencia de inteligencia privada fundada en 2010 por exagentes israelíes, con sedes en Tel Aviv, Londres y Madrid, se especializa en inteligencia para litigios, recopi-

Además, el auge de los cibermercenarios o los grupos de ransomware... ha comercializado la ciberguerra. Estos actores no estatales pueden ser contratados por naciones o corporaciones o actuar de forma independiente... lo cual hace que se difumine la línea entre la actividad estatal y la delictiva.

4 Jeff Kosseff (2019). "The Contours of 'Defend Forward' Under International Law". *CCDCOE (Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN)*. [https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf]

5 "NATIONAL CYBERSECURITY STRATEGY". March 2023. [https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf]

6 MITRE ATT&CK MATRIX FOR ENTERPRISE (2022). [https://attack.mitre.org/matrices/enterprise]

7 Cybersecurity and Infrastructure Security Agency. "CISA and Partners Release Advisory on Akira Ransomware". [https://www.cisa.gov/news-events/alerts/2024/04/18/cisa-and-partners-release-advisory-akira-ransomware]

8 NSO Group. [https://www.nsogroup.com].

9 Black Cube. [https://www.blackcube.com]

En paralelo, ha surgido un mercado clandestino de exploits y datos robados... La convergencia entre intereses estatales, económicos y delictivos ha generado un ecosistema donde la colaboración y el intercambio de técnicas son comunes.

lando pruebas y rastreando activos, combinando agentes de campo e inteligencia cibernética. Ha estado envuelta en controversias por investigar a denunciantes de Harvey Weinstein y por operaciones de espionaje político.

Entre 2023 y 2025 se ha visto el ascenso de la Alianza Intellexa (un consorcio de empresas vinculadas al desarrollo y la comercialización de software espía comercial) y su *spyware* Predator. Investigaciones forenses realizadas por Citizen Lab y Amnesty International han desvelado la sofisticación técnica y el alcance de esta amenaza[10].

A principios de 2024, CISA, la NSA y el FBI emitieron alertas conjuntas sobre Volt Typhoon, un actor patrocinado por la República Popular China. Este grupo representa un cambio doctrinal en la estrategia cibernética china, que se aleja del robo de propiedad intelectual y dirige su atención a la preparación operativa para el conflicto militar[11].

En paralelo, ha surgido un mercado clandestino de *exploits* y datos robados, que permite que incluso actores con recursos limitados puedan acceder a capacidades avanzadas. Alianza Intellexa utilizó una cadena de *exploits* de día cero (se refiere a fallas aún desconocidas) en iOS (CVE-2023-41991, CVE-2023-41992, CVE-2023-41993) para escalar privilegios (obtener acceso a funciones restringidas del sistema) y ejecutar código arbitrario (hacer que el sistema ejecute instrucciones del atacante), demostrando capacidades técnicas a la par de las agencias de inteligencia de primer nivel[12]. La convergencia entre intereses estatales, económicos y delictivos ha generado un ecosistema donde la colaboración y el intercambio de técnicas son comunes, lo cual incrementa la complejidad de la defensa y la necesidad de estrategias flexibles y adaptativas.

Google Threat Analysis Group (TAG), en "Buying Spying: How the commercial surveillance industry works and what can be done about it" (2024), ofrece una visión técnica y de mercado sobre los cibermercenarios. Explica cómo estas empresas desarrollan y venden herramientas de hackeo a operadores gubernamentales y no gubernamentales, y cómo sus acciones ponen en riesgo la seguridad de internet. El documento clasifica los tipos de actores y las cadenas de explotación que utilizan en función de la inteligencia de amenazas recopilada por Google[13].

Esta diversificación de actores y tácticas ha obligado a los estados a desarrollar capacidades más sofisticadas de ciberinteligencia y respuesta. Los marcos legales internacionales se ven cada vez más desafiados para adaptarse a la velocidad y al anonimato de estos ataques, mientras que la atribución precisa de estos se convierte en un reto técnico y diplomático considerable. Así, la disuasión y la resiliencia digital pasan a ser elementos prioritarios en la planificación de la seguridad nacional, por lo que promueven inversiones en infraestructura cibernética, formación de especialistas y cooperación global para hacer frente a amenazas multidimensionales.

El campo de batalla ampliado: infraestructura crítica y guerra cognitiva

En el artículo de 2007 se identifica la infraestructura como un objetivo clave. Sin embargo, la realidad ha resultado más alarmante que el riesgo teórico de 2007. Eventos posteriores al artículo han demostrado las consecuencias tangibles y reales de los ciberataques a sistemas críticos:

Stuxnet (2010): Este sofisticado gusano, ampliamente atribuido a un esfuerzo conjunto entre Estados Unidos e Israel, dañó físicamente centrifugadoras nucleares iraníes mediante la manipulación de los sistemas de control industrial (ICS, por sus siglas en inglés). Este evento histórico demostró que un arma digital podía causar efectos cinéticos.

10 "To Catch a Predator: Leak exposes the internal operations of Intellexa's mercenary spyware" (2025). *The Security Lab*. [https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed]

11 "PRC STATE-SPONSORED CYBER ACTIVITY: Actions for Critical Infrastructure Leaders" (2024). [https://www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c_0.pdf]

12 Google Threat Intelligence Group (2025). "Sanctioned but Still Spying: Intellexa's Prolific Zero-Day Exploits Continue". [https://cloud.google.com/blog/topics/threat-intelligence/intellexa-zero-day-exploits-continue]

13 Google's Threat Analysis Group (TAG). [https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf?utm_source=chatgpt.com]

The Shamoon-Attack I y II (2012): El 15 de agosto de 2012, Saudi Aramco debió aislar su red informática tras un ataque con *malware* Disttrack, que afectó a 35.000 computadoras y puso en riesgo el suministro del 10 % del petróleo mundial. El virus se propagó en la red y borró archivos antes de reescribir el *Master Boot Record*, dejando a la empresa una semana sin servicios. Aunque EE. UU. señaló a Irán como responsable, no hay pruebas concluyentes; ambos países mantienen tensiones ideológicas y geopolíticas desde 1979.

Yellowstone 1 (2014): En 2014, hackers presuntamente iraníes atacaron el casino Las Vegas Sands Corp. en represalia por *declaraciones* polémicas de su CEO sobre Irán. El ataque, realizado mediante una "bomba de malware" que abusó de las credenciales de un empleado, paralizó gran parte de los sistemas informáticos de la empresa en Las Vegas, lo cual afectó servidores, correos electrónicos, teléfonos y operaciones tecnológicas clave.

Ataques a la red eléctrica de Ucrania (2015-2016): Hackers rusos respaldados por el Estado lograron desconectar partes de la red eléctrica de Ucrania y dejaron a cientos de miles de personas sin electricidad en pleno invierno[14].

Ataque de *ransomware* al oleoducto Colonial (2021): El ataque de *ransomware* de un grupo criminal contra un importante operador de oleoductos de EE. UU. provocó escasez de combustible en la Costa Este, lo que demuestra la vulnerabilidad de la infraestructura privada ante actores no estatales y el potencial de una disrupción social generalizada[15].

Más allá de la infraestructura física, la nueva frontera es la guerra cognitiva. Si bien el artículo original de 2007 aborda la guerra psicológica a través de internet, el enfoque moderno es más sistémico. Implica el uso de redes sociales, *deepfakes* y campañas coordinadas de desinformación para erosionar la confianza pública, polarizar las sociedades e influir en los procesos democráticos, lo cual convierte el propio espacio informativo en un dominio disputado.

Según Irene Pujol (2024), la guerra cognitiva es un nuevo dominio de conflicto donde la mente humana es el campo de batalla. Sostiene que, en lugar de la fuerza física, se utilizan la psicología y la tecnología para manipular la percepción e influir en la toma de decisiones. Aprovecha los "atajos mentales" y los sesgos cognitivos del cerebro para alcanzar objetivos estratégicos sin recurrir a la acción militar convencional, lo cual destaca la necesidad de entender y abordar las vulnerabilidades de nuestro sistema cognitivo[16].El reconocimiento de estas vulnerabilidades es crucial en la era de la guerra cognitiva, ya que la defensa efectiva no solo requiere proteger sistemas tecnológicos, sino también fortalecer la capacidad de análisis crítico y resiliencia psicológica de la sociedad frente a intentos de manipulación masiva.

Según Irene Pujol (2024), la guerra cognitiva es un nuevo dominio de conflicto donde la mente humana es el campo de batalla... utilizan la psicología y la tecnología para manipular la percepción e influir en la toma de decisiones.

Así como los hackers tradicionales buscan errores de software para acceder a sistemas, quienes practican el "hacking humano" se enfocan en identificar y manipular esos "atajos mentales" y sesgos cognitivos que guían nuestras decisiones cotidianas. Estos sesgos, como la tendencia a confiar en la información repetida o a seguir la opinión mayoritaria, funcionan como verdaderas "puertas traseras" cognitivas que pueden explotarse para influir en el comportamiento, la percepción y la toma de decisiones de individuos o grupos.

Asimismo, la Organización de Ciencia y Tecnología de la OTAN (NATO STO) ha elevado la Guerra Cognitiva (*Cognitive Warfare* o *CogWar*) a la categoría de desafío de investigación estratégica. A diferencia de las operaciones psicológicas (*PsyOps*) o la guerra de información tradicional, que se centran en el control del flujo de información, la guerra cognitiva se define como "el arte de utilizar tecnologías para alterar la cognición de objetivos humanos".

François du Cluzel, del Centro de Innovación del Comando Aliado de Transformación (ACT) de la OTAN, establece en sus informes de 2021 y en actualizaciones posteriores

14 Gazula Mohan B. (2017). "Cyber Warfare Conflict Analysis and Case *Studies, Cybersecurity Interdisciplinary Systems Laboratory (CISL)". Sloan School of Management, Room E62-422. Massachusetts Institute of Technology.*

15 "Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack" (2021). *The Guardian*. [https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom]

16 Irene Pujol (2024). "La guerra cognitiva convierte la mente en un campo de batalla". *Revista Española de Defensa*, p. 48.

El Microsoft Digital Defense Report 2024 revela que Microsoft analiza más de 78 billones de señales de seguridad diariamente... lo que permite identificar patrones de ataque sutiles y activar mecanismos de "interrupción automática de ataques".

que el objetivo ya no es simplemente engañar, sino "hackear al humano", aprovechando las vulnerabilidades inherentes del cerebro[17].

Como conclusión, la sofisticación de estas tácticas cognitivas se ha visto incrementada por la automatización y el uso de inteligencia artificial, que permiten segmentar audiencias con precisión, adaptar mensajes en tiempo real y amplificar narrativas a gran escala. De este modo, los adversarios no solo buscan sabotear infraestructuras, sino manipular percepciones colectivas y provocar respuestas sociales predecibles para afectar la cohesión interna de los países objetivo. Así, la defensa ya no solo debe proteger sistemas físicos o digitales, sino también blindar al tejido social frente a ataques que explotan la psicología y la información. De este modo, se consolida la guerra cognitiva como eje central en la competencia entre estados y actores no estatales.

IA y automatización: el futuro del ciberconflicto

La inteligencia artificial (IA) está transformando la naturaleza de la ciberguerra. Tanto atacantes como defensores están aprovechando estas tecnologías para automatizar y acelerar sus operaciones.

La IA se puede usar para crear *malware* altamente adaptable, que cambia su código para evadir la detección, realizar reconocimientos automatizados de redes objetivo y ejecutar ataques también automatizados que identifican y explotan vulnerabilidades en tiempo real. El informe de BlackBerry Global Threat Intelligence 2024 reportó un aumento del 40 % por minuto en la aparición de nuevos *hashes* de *malware* únicos (código único que identifica un archivo o programa), un volumen que sugiere fuertemente el uso de automatización e IA en el desarrollo[18, 19].

Por otro lado, la IA permite detectar patrones anómalos en grandes volúmenes de tráfico, anticipar movimientos maliciosos y responder a incidentes con mayor rapidez y precisión.

El Microsoft Digital Defense Report 2024 revela que Microsoft analiza más de 78 billones de señales de seguridad diariamente. Esta capacidad de procesamiento masivo permite identificar patrones de ataque sutiles (como el movimiento lateral de credenciales o programación del atacante dentro de una red comprometida) y activar mecanismos de "interrupción automática de ataques" (*automatic attack disruption*), aislando dispositivos comprometidos en tiempo real antes de que el atacante pueda desplegar un *ransomware*, por ejemplo. La batalla futura será "la IA contra la IA": algoritmos ofensivos buscando brechas contra algoritmos defensivos cerrándolas en milisegundos[20].

El despliegue de sistemas inteligentes en ambos frentes está redefiniendo el ritmo y la escala del ciberconflicto. Esto provoca que las amenazas evolucionen constantemente y obliga a las organizaciones a invertir en tecnologías de vanguardia y actualización continua de sus capacidades. En este escenario, la automatización y el aprendizaje automático se posicionan como herramientas indispensables tanto para la protección de infraestructuras críticas como para la gestión eficaz de la guerra cognitiva y la defensa nacional.

Conclusiones

El análisis presentado a lo largo de este artículo evidencia que la evolución del ciberconflicto ha dejado de ser un fenómeno marginal o estrictamente técnico para convertirse en un eje central de las relaciones internacionales contemporáneas. Los ejemplos históricos —desde Stuxnet y los ataques a la red eléctrica de Ucrania hasta el *ransomware* que afectó al oleoducto Colonial— demuestran que tanto actores estatales como no estatales cuentan hoy con la capacidad de provocar daños físicos, disrupciones económicas y crisis sociales a través del ciberespacio. Estos incidentes no solo revelan la vulnerabilidad de infraestructuras críticas, sino que subrayan la creciente so-

17 François du Cluzel (2021). "Cognitive warfare". [https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf?utm_source=chatgpt.com]

18 "BlackBerry Reports 40 Percent Increase in New Malware Used in Cyberattacks" (2024). *PR Newswire Amplify*. [https://www.prnewswire.com/news-releases/blackberry-reports-40-percent-increase-in-new-malware-used-in-cyberattacks-302181233.html?utm_source=chatgpt.com]

19 Allyson M. Morris (2025). "Detecting Generative-AI-Enabled Polymorphic Malware: A Semantic-Behavior Approach". *College of William & Mary Williamsburg*, Virginia, EE. UU. [https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1134&context=covacci-undergraduateresearch]

20 Microsoft Threat Intelligence (2024). "10 essential insights from the Microsoft Digital Defense Report". [https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/10-essential-insights-from-the-microsoft-digital-defense-report-2024]

fisticación y creatividad de los adversarios, quienes aprovechan la interconectividad global para ejecutar operaciones con consecuencias concretas y, muchas veces, impredecibles.

Sin embargo, el artículo trasciende el análisis de la infraestructura física y se adentra en la que probablemente sea la nueva frontera de la guerra: el dominio cognitivo. La guerra cognitiva, impulsada por la masificación de las redes sociales, la aparición de *deepfakes* y el desarrollo de campañas de desinformación, representa una amenaza que no se dirige únicamente a sistemas técnicos, sino directamente al núcleo de la cohesión social y la confianza pública. En este sentido, la manipulación de percepciones, la polarización política y la erosión de la legitimidad democrática se han convertido en objetivos estratégicos de primer orden para actores que buscan ventajas sin recurrir a la violencia tradicional.

¿Qué hacer entonces? La resiliencia social y la "alfabetización digital" se han convertido en la nueva "armadura" indispensable para el ciudadano moderno frente a los desafíos del ciberespacio. En un entorno donde la manipulación informativa y los ataques cognitivos buscan explotar debilidades colectivas, fortalecer la capacidad de discernimiento crítico y adaptabilidad social es fundamental para resistir intentos de desinformación y polarización.

La alfabetización digital no se limita a manejar herramientas tecnológicas, sino que implica comprender los riesgos, identificar noticias falsas, proteger los datos personales y participar activamente en la construcción de una cultura digital ética y responsable. Así, una sociedad resiliente y educada digitalmente tiene mayor capacidad para anticipar amenazas, responder de manera coordinada y preservar la cohesión social y, de ese modo, blindar los valores democráticos ante la constante evolución del ciberconflicto.

... la IA permite la creación de malware evolutivo y ataques automatizados capaces de adaptarse y evadir defensas en tiempo real. Por el otro, dota a los equipos de ciberseguridad de herramientas capaces de analizar grandes volúmenes de datos...

El empleo de inteligencia artificial y la automatización han potenciado exponencialmente la efectividad de estas tácticas. Por un lado, la IA permite la creación de *malware* evolutivo y ataques automatizados capaces de adaptarse y evadir defensas en tiempo real. Por el otro, dota a los equipos de ciberseguridad de herramientas capaces de analizar grandes volúmenes de datos, detectar anomalías y responder con rapidez y precisión. Este pulso tecnológico ha acelerado el ritmo del ciberconflicto y plantea un desafío constante a los Estados, las empresas y los ciudadanos: la necesidad de invertir en capacidades de vanguardia y en la actualización continua de sus estrategias y conocimientos.

Las implicaciones de esta transformación son profundas. La defensa nacional ya no puede limitarse a la protección de fronteras físicas o sistemas digitales; debe, además, blindar al tejido social frente a ataques que explotan la psicología colectiva y la información. Asimismo, la cooperación internacional, el intercambio de inteligencia y la formulación de marcos legales y éticos robustos se tornan imprescindibles para enfrentar amenazas que, por naturaleza, trascienden jurisdicciones y desafían los paradigmas clásicos de soberanía.

Finalmente, la ciberguerra, tal como se describe en el artículo, es un terreno en constante evolución, donde la línea entre ataque y defensa es cada vez más difusa. Los Estados deben adoptar una postura proactiva, combinando "defensa avanzada" y "compromiso persistente" para anticipar y neutralizar amenazas antes de que se materialicen en daños reales, como lo subraya la estrategia del Departamento de Defensa de EE. UU. y los planteamientos de líderes como el General Nakasone. Sin embargo, la verdadera clave residirá en la capacidad de adaptarse, innovar y comprender que la competencia en el ciberespacio es permanente, multidimensional y, sobre todo, profundamente humana.

En suma, la ciberseguridad y la defensa nacional del siglo XXI exigen una visión integral, proteger infraestructuras, fortalecer capacidades técnicas y, sobre todo, blindar a la sociedad frente a la manipulación y la desinformación. Solo así será posible preservar la estabilidad, la democracia y la confianza en un entorno global cada vez más interconectado y disputado. ■