LIBERTAD DE ACCIÓN EN EL CIBERESPACIO

Carlos García-Trejo Arnedo
Comandante de Transmisiones, Cuerpo General del Ejército de Tierra (CGET)
España

RESUMEN

La Publicación Doctrinal Conjunta de Operaciones en el Ámbito Ciberespacial (PDC-3.20) señala que la libertad de acción en el ciberespacio resulta un factor fundamental en la ejecución de las operaciones. La estrategia de ciberdefensa adoptada por un país es la piedra angular sobre la que se alcanza y mantiene la libertad de acción en el ciberespacio. En 2018, EE.UU., una de las mayores superpotencias en dicho ámbito, modificó de forma drástica su estrategia de ciberdefensa. Hasta ese momento, su estrategia había estado centrada en la disuasión y la protección de las ciber infraestructuras; sin embargo, la nueva estrategia era mucho más proactiva, buscando disputar a los potenciales adversarios el dominio del ciberespacio de manera continuada y llevar esta disputa lo más cerca posible de los adversarios. Este trabajo pretende analizar la eficacia de la nueva estrategia de ciberdefensa adoptada por EE.UU. en 2018.

Palabras clave:

ciberdefensa, libertad de acción, ciberespacio, ciberseguridad, defend forward, persistent engagement.

ABSTRACT

PDC 3.20 points out that freedom of action in cyberspace is a fundamental factor in the execution of operations. The cyber defense strategy adopted by a country is the cornerstone on which freedom of action in cyberspace is achieved and maintained. In 2018, the U.S., one of the major superpowers in that field, drastically modified its cyber defense strategy. Until that time, its strategy had been focused on deterrence and protection of cyber infrastructures; however, the new strategy, was much more proactive, seeking

to contest potential adversaries for the dominance of cyberspace on an ongoing basis and to bring this dispute as close as possible to the adversaries. This paper aims to analyze the effectiveness of the new cyber defense strategy adopted by the U.S. in 2018

Key Words:

cyber defense, cybersecurity, freedom of action, cyberspace, cybersecurity, defend forward, persistent engagement.

INTRODUCCIÓN

El término “cibernética” fue introducido por el filósofo estadounidense Norbert Wiener en 1948 para hacer referencia a la interacción entre humanos y máquinas (Ottis, 2008), pero no fue hasta 34 años más tarde cuando apareció el término “ciberespacio”. En 1982, el escritor norteamericano William Gibson empleo este término en su novela corta “Burning Chrome” y en 1984 lo volvió a emplear de nuevo en su aclamada novela “Neuromancer”, el autor empleó el término para referirse a la percepción humana de un nuevo entorno de marcada complejidad (Ottis y Lorents, 2010). Con posterioridad se han desarrollado un gran número de definiciones, abordando el término desde diferentes perspectivas; la mayoría de ellas coinciden en que el ciberespacio está formado por redes de hardware, software y datos conectadas globalmente, con las que los seres humanos pueden interactuar.

Desde su origen, el ciberespacio se ha constituido como una de las dimensiones de los conflictos, junto con el terrestre, el aeroespacial y el marítimo, aunque su reconocimiento oficial como tal llegó posteriormente. EE.UU. reconoció el ciberespacio como un dominio de operaciones en 2004, pero la OTAN no lo reconoció hasta la cumbre de Varsovia en 2016. En el comunicado tras la cumbre, los jefes de estado se expresaron del siguiente modo: "En Gales acordamos que la ciberdefensa forma parte de la tarea central de la OTAN de Defensa colectiva. Ahora, en Varsovia, reafirmamos el mandato defensivo de la OTAN, y reconocemos el ciberespacio como un dominio de operaciones en el que la OTAN debe defenderse tan eficazmente como lo hace en el aire, en tierra y en el mar." (NATO Warsaw Summit Communiqué, 2016).

Las singulares características del ciberespacio lo hacen completamente diferente a cualquiera de los dominios “convencionales”. Es un ámbito artificial

compuesto por infraestructuras, redes, y sistemas de información y telecomunicaciones que evoluciona rápidamente creando oportunidades y vulnerabilidades de forma continua. Es transversal a los demás ámbitos, de modo que las acciones en el ciberespacio pueden manifestarse en los demás dominios. La ausencia de límites o fronteras, el anonimato, su fácil acceso, la inmediatez y su infinita extensión son otras de sus principales características (PDC-01(A), 2018). A las que habría que sumar las que le atribuye Estrategia Nacional de Seguridad de 2019: ausencia de soberanía y débil jurisdicción (Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional). Estas características lo convierten en el principal dominio de competición en la zona gris del conflicto.

La opinión predominante entre los pensadores militares contemporáneos es que la "libertad de acción" es imprescindible para llevar a cabo operaciones en todos los niveles, desde el táctico al estratégico (López 1952). Cuando la OTAN declaró el ciberespacio un dominio de operaciones, reconoció de forma implícita la necesidad de conseguir y mantener la libertad de acción en él. El preámbulo de la publicación doctrinal nacional conjunta para las "Operaciones en el Ámbito Ciberespacial" (PDC-3.20) comienza del siguiente modo "la libertad de acción en el ciberespacio resulta un factor fundamental en la ejecución de las operaciones…." (PDC 3.20, 2021, pp.13).

Tanto la doctrina OTAN como la nacional catalogan las operaciones en el ciberespacio como ofensivas o defensivas. Según ambos documentos doctrinales, las operaciones defensivas (DCO) tienen como objetivo principal preservar la capacidad de utilizar el ciberespacio, garantizando así nuestra propia libertad de acción; en consecuencia, se enfocan en la protección para hacer frente a las acciones de los adversarios. Sin embargo, las operaciones ofensivas (OCO) están orientadas a la consecución de objetivos militares a través de acciones (AJP-3.20, 2020). En resumen, se podría concluir que la finalidad de las operaciones defensivas sería conseguir y mantener la libertad de acción propia, mientras que la de las operaciones ofensivas sería alcanzar objetivos militares

La palabra "estrategia" puede definirse según la Real Academia Española como "el conjunto de reglas que buscan la decisión óptima en cada momento"; por lo tanto una estrategia de ciberdefensa puede entenderse como el modo en el que se emplearán las operaciones en el ciberespacio junto con otros recursos auxiliares, para conseguir y mantener la libertad de acción en dicho ámbito. En definitiva, la estrategia de ciberdefensa será la herramienta que emplearemos para conseguir y mantener la "libertad de acción".

EXPOSICIÓN

Hasta hace cinco años, casi todos los países del mundo basaban la protección de sus redes en estrategias de ciberdefensa defensivas/reactivas. Durante el último lustro, algunos países han abandonado esta estrategia, este es el caso de EE.UU., Reino Unido e Israel. En el caso de los EE.UU., los ciberataques sufridos entre 2012 y 2018, y las injerencias de terceros países en sus procesos electorales, hicieron que se dieran cuenta de que las políticas defensivas/reactivas complementadas con el empleo de diferentes tipos de disuasión no eran efectivas en el ámbito ciberespacial (Goldsmith, 2022).

Las elecciones presidenciales de EE.UU. de 2016 marcaron un punto de inflexión en la estrategia de ciberdefensa estadounidense debido al gran impacto de las injerencias de terceros países en las mismas. Rusia intentó influir en las elecciones a través de una campaña que incluía el ciber espionaje contra los partidos políticos, el pirateo de juntas electorales y una extensa campaña propagandística. Su objetivo era perjudicar a la candidata demócrata, favorecer al republicano e incrementar la tensión política y social en EE.UU.

La estrategia de ciberdefensa empleada por EE.UU. en 2016 estaba centrada en la disuasión, potenciando principalmente el aspecto defensivo. Esta estrategia, impulsada por la administración Obama, se apoyaba en la "Estrategia Internacional para el Ciberespacio" publicada por la Casa Blanca en 2011. El documento afirmaba que "Estados Unidos, junto con otras naciones, fomentará un comportamiento responsable y se opondrá a quienes pretendan perturbar las redes y los sistemas, disuadiendo y desalentado a los actores maliciosos… " (International Strategy for Cyberspace , 2011, pp.8). Este documento hacía hincapié en reforzar la disuasión por denegación[1], y por ende ponía de manifiesto su intención de reforzar el aspecto defensivo, de supervivencia y de resiliencia de los sistemas estadounidenses en el ciberespacio.

Estos mismos principios se plasmaron en la Estrategia de Ciberdefensa publicada por el Departamento de Defensa (DoD) en 2015, reafirmando el enfoque centrado en la defensa y la disuasión, desestimando el empleo de acciones ofensivas: "… en principio, EE.UU. tratará de agotar todas las opciones de defensa … y de aplicación de la ley para mitigar cualquier riesgo potencial para la nación o los intereses de EE.UU. antes de llevar a cabo una operación en el ciberespacio" (DoD Cyber Strategy, 2015, pp. 5), comprometiéndose a "realizar siempre operaciones bajo la doctrina de la moderación" (DoD Cyber Strategy, 2015, pp. 6).

Según el informe del fiscal responsable de la investigación de las injerencias rusas en las elecciones presidenciales de 2016, Rusia empleó la Internet Research Agency (IRA)[2] para llevar a cabo una campaña en redes sociales para favorecer al candidato republicano y dañar la imagen de la candidata demócrata (Mueller Report, 2019). La campaña de desinformación en las redes sociales no permitía a EE.UU. hacer un uso libre del ciberespacio bajo su soberanía, y por lo tanto constreñía su libertad de acción. La estrategia de ciberdefensa vigente (reactiva) no permitió a EE.UU. realizar acciones contra la IRA. Aún en el caso de haber tenido la capacidad de actuar contra ella, el resultado de sus actuaciones habría estado condicionado por la falta de conocimiento de la red objetivo. Otra de las debilidades de la estrategia de ciberdefensa que se puso de manifiesto en las elecciones de 2016 fue la falta de coordinación y colaboración entre el sector público y el privado.

Esta estrategia tampoco pudo proteger de forma eficaz las redes ante los ciberataque perpetrados por el el servicio de inteligencia ruso (GRU). El GRU exfiltró información del Partido Demócrata y de cuentas de correo electrónico de personas involucradas en la campaña presidencial de Clinton. La información obtenida se publicó estratégicamente de forma gradual durante la campaña para desviar la atención de acontecimientos que favorecían o perjudicaban a los candidatos.

Del análisis de los ciberataques realizados contra los partidos se puede inferir que el GRU disponía de la capacidad de exfiltrar información de las redes atacadas con anterioridad al desarrollo de las elecciones. Este hecho pone de manifiesto que las medidas de protección aplicadas por las estrategias reactivas no son lo suficientemente robustas cuando se enfrentan a un enemigo persistente que conduce ciber operaciones de forma continuada con el objeto de comprometer redes específicas. La pasividad de estas estrategias de ciberdefensa permiten al atacante realizar numerosas pruebas de ensayo y error hasta que alcanzan sus objetivos. Esta pasividad permite que el adversario pueda empeñar todos sus recursos en el objetivo, sin tener que reservar recursos para proteger sus propias redes.

Otra de las debilidades de las estrategias reactivas identificadas como consecuencia de los ataques rusos fue que las medidas de defensa implementadas en las redes de las empresas privadas no eran efectivas. Los sistemas de protección aplicados a las empresas privadas se alimentan de librerías o repositorios de software malicioso (malware) detectado en las redes públicas. Cuando el malware se desarrolla para atacar una red específica y se emplea por primera vez, es muy difícil que sea detectado por los sistemas de monitorización convencionales. Las estrategias reactivas no realizan un búsqueda activa de malware en redes de potenciales adversarios, y por lo tanto no son capaces de protegerse ante amenazas avanzadas persistentes.

La campaña de actuaciones de los piratas informáticos rusos fue tan agresiva, que el presidente Obama decidió contactar directamente con el presidente ruso a través de la línea directa para advertirle de que los ciberataques corrían el riesgo de desencadenar una escalada (Riley y Robertson, 2017). Esta reacción del presidente estadounidense para detener la injerencia de Rusia en las elecciones es una muestra de la pérdida total de la libertad de acción de EE.UU., y de la incapacidad de hacer frente a las operaciones contra sus redes. En definitiva, pone de manifiesto la ineficacia de la estrategia de ciberdefensa empleada.

La injerencia de Rusia en las elecciones presidenciales de 2016 derrumbaron toda la visión del presidente Obama centrada en la disuasión y la desescalada. La incapacidad de la administración para disuadir y responder eficazmente a las operaciones rusas durante las elecciones presidenciales colapsaron la estrategia defensiva desarrollada hasta ese momento; el ex jefe de gabinete del presidente Obama, Denis McDonough, señaló que: "es lo más difícil de defender de todo el tiempo que llevo en el Gobierno" (Miller et al., 2017, pp.na). El viceconsejero de seguridad nacional de Obama, Ben Rhodes, fue el que quizás mejor interpretase el porqué del fracaso de esta estrategia: "... nos enfrentamos a esto como una amenaza en el ciberespacio y nos centramos en proteger nuestra infraestructura. Mientras tanto, los rusos estaban jugando a algo mucho mayor, que incluía elementos como la publicación de material robado, propaganda política y propagación de noticias falsas… " (Miller et al., 2017, pp. na).

La injerencia en las elecciones presidenciales de 2016 sirvió para que EE.UU. aprendiese las tácticas y técnicas empleadas por Rusia para llevar a cabo sus campañas de injerencia. En respuesta, EE.UU. se preparó minuciosamente para proteger las elecciones de mitad de mandato de 2018 contra las operaciones rusas.

A comienzos de 2018 el USCYBERCOM presentaba su visión estratégica; esta visión suponía un cambio de ciento ochenta grado en la estrategia de ciberdefensa estadounidense. Se abandonaba la postura defensiva/reactiva centrada en la disuasión para pasar a una postura mucho más agresiva que le permitiese anticiparse a las acciones de sus adversarios. Esta nueva estrategia empleaba como herramientas principales los conceptos “Defend Forward” y “Persistent Engagement”. El concepto “Defend Forward”, implicaba adoptar una actitud más proactiva en el ciberespacio, llevando a cabo acciones de protección a vanguardia de las redes propias con el objeto de neutralizar las amenazas lo más lejos posible de los sistemas propios. El segundo concepto era el de “Persistent Engagement”, que implicaba combatir de forma permanente la actividad maliciosa en el ciberespacio (U.S. Cyber Command, 2018). Además, este cambio en la estrategia fue acompañado de las

pertinentes transformaciones legislativas y ejecutivas que habilitaban al USCYBERCOM a poner en práctica la nueva estrategia de manera óptima.

Cuando el General Nakasone tomó el timón de la NSA y el USCYBERCOM en mayo de 2018, el entonces secretario de Defensa, Jim Mattis, le ordenó que su prioridad debía ser la defensa de las elecciones de mitad de mandato. El ejecutivo no quería que se repitiera lo que sucedió en 2016 (Nakashima, 2019b).

El concepto “Defend Forward” se puso a prueba de inmediato. Como parte de los esfuerzos del gobierno estadounidense para proteger las elecciones, en junio de 2018, el general Paul Nakasone, emprendió una iniciativa denominada Russia Small Group (RSG). El RSG[3] era una iniciativa que pretendía integrar los esfuerzos gubernamentales con el de las entidades privadas para defender las elecciones de la interferencia e influencia extranjeras. Implicó una serie de operaciones innovadoras en apoyo de acciones más amplias del gobierno estadounidense, incluidas CO ofensivas discretas para interrumpir el uso activo de las capacidades ciber por parte de Rusia (Corn, 2022).

El RSG colaboró con países aliados y con el sector privado para aumentar su eficacia; compartiendo información directamente con la industria para que pudiera desarrollar contramedidas. La coordinación y cooperación que se materializó a través del RSG, permitió actuar de forma coordinada para mejorar la protección de las redes susceptibles de ser atacadas, disminuyendo en gran medida la eficacia de los ataque dirigidos contra ellas.

Que el USCYBERCOM operara en las redes del adversario le permitió contratacar con su propia campaña de información para influir en las organizaciones rusas implicadas. El USCYBERCOM envió mensajes directos dirigidos a los trolls de la IRA, así como a los hackers que trabajan para la agencia de inteligencia militar rusa (GRU). A través de correos electrónicos, ventanas emergentes, mensajes de texto o mensajes directos, los agentes estadounidenses hicieron saber a los rusos que conocían sus nombres reales y sus cuentas en Internet y que no debían interferir en los asuntos de otros países (Nakashima, 2019a; Barnes, 2018b).

Estas acciones para contrarrestar la campaña de influencia rusa no hubieran sido posibles de no ser por la nueva estrategia de ciberdefensa. Operar en las redes del adversario, obteniendo información para utilizarla de forma oportuna, obligó al adversario a empeñar parte de sus recursos en la protección de sus propias redes, coartando de este modo su libertad de acción y favoreciendo la propia.

Ante la campaña rusa, el USCYBERCOM ejecutó un ciberataque contra la IRA (Nakashima, 2019a). En los días previos a que se celebrasen las elecciones, considerados cruciales para el desarrollo de las mismas, el USCYBERCOM llevó a cabo una serie de operaciones disruptivas contra la Agencia de Investigación de Internet (IRA) y otras entidades ciber-rusas que logró interrumpir el acceso de la IRA a Internet durante una fase crucial de las elecciones, y por lo tanto, interrumpieron su campaña de desinformación e interferencia.

Las OCO formaron una pieza central de los esfuerzos liderados por el RSG para proteger las elecciones de mitad de período de 2018. Estas operaciones no habrían sido posibles sin el marco legal necesario. A este fin, contribuyeron de forma decisiva las disposiciones estatutarias específicas para el ciberespacio contempladas en la Ley de Autorización de Defensa Nacional que categorizaron las OCO como actividades militares tradicionales y por lo tanto exentas de largos procedimientos de aprobación y supervisión.

La protección de las elecciones de 2018 supuso la primera prueba relevante para la nueva estrategia de ciberdefensa. El general Nakasone calificó la prueba como un éxito, al probar y demostrar la necesidad de defender las redes lo más cerca posible del adversario. El general Nakasone afirmó que "Persistent Engagement" limitó la libertad de acción de los adversarios al tiempo que permitió a los EE.UU. mantener una posición ventajosa en los enfrentamientos, favoreciendo por tanto su libertad de acción. El cambio de estrategia de ciberdefensa fue decisivo para proteger con éxito las elecciones de 2018 de la interferencia de terceros países. La valoración por parte del USCYBERCOM era que con la nueva estrategia se estaba combatiendo a los adversarios con sus mismas armas, y por lo tanto en igualdad de condiciones (Nakashima, 2019).

Las operaciones de injerencia extranjeras volvieron a estar presentes en las elecciones de 2020, buscando denigrar la candidatura del presidente Biden y al Partido Demócrata, apoyar al expresidente Trump, socavar la confianza pública en el proceso electoral y exacerbar las divisiones sociopolíticas en EE.UU. (Intelligence Community Assessment: Foreign Threats to the 2020 US Federal Elections, 2021)

En el año 2020, la estrategia de ciberdefensa "Defend Forward" estaba completamente implantada y el gobierno estadounidense la había dotado de los medios, herramientas y mecanismos necesarios para asegurar su efectividad. La protección de las elecciones de 2018 sirvieron al USCYBERCOM para ganar experiencia y poner en práctica los nuevos conceptos.

Si en 2016 Rusia sorprendía a EE.UU. por las técnicas empleadas durante las elecciones, y en 2018 eran los EE.UU. los que sorprendían a sus adversarios por el cambio radical de su estrategia; en 2020, tanto EE.UU. como sus potenciales adversarios conocían cuales serían las técnicas empleadas durante la elecciones presidenciales. De modo, que en caso de tener éxito, las elecciones de 2020 servirían a EE.UU. para validar la eficacia de su estrategia de ciberdefensa.

La puesta en práctica de “Persistent Engagement” desde 2018, permitió al USCYBERCOM adquirir experiencia y aprender sobre la inteligencia, las capacidades, el personal y los socios necesarios para obtener y mantener la libertad de acción en el ciberespacio. Las lecciones aprendidas por el RSG en 20018 definieron la composición y las tareas del grupo de trabajo que le sucedió, el Grupo de Seguridad Electoral (ESG). Como explicó el general Nakasone al Congreso en marzo de 2020: "El año pasado institucionalizamos nuestros esfuerzos del RSG antes de las elecciones de 2018 en un Grupo de Seguridad Electoral permanente para las elecciones de 2020 y las siguientes" (Nakasone, 2020).

Otra de las características de la estrategia “Defend Forward” que se impulsaron entre 2018 y 2020 fueron las operaciones “Hunt Forward”[4]. Durante las “misiones de caza”, los equipos del USCYBERCOM buscaron malware e indicadores de riesgo en las redes de países aliados. La información obtenida sirvió para mejorar su defensa nacional y la de países aliados y amigos. El General Nakasone resumió el valor de estas operaciones: "El efecto neto de las numerosas misiones de caza de malware que el USCYBERCOM ha realizado en los últimos años ha sido la “vacunación” masiva de millones de sistemas, lo que ha reducido la eficacia del malware desarrollado por nuestros adversarios" (Nakasone, 2020b).

Para contrarrestar las operaciones de influencia en las redes sociales, el ESG contó con la inestimable colaboración de las empresas privadas. Si en 2016 las empresas eran reticentes a reconocer que sus plataformas se estaban empleando para influenciar las elecciones, en 2020 eran ellas las que monitorizaban y denunciaban tales comportamientos. Desde 2016 a 2020 se había mejorado la colaboración y la coordinación entre el sector público y privado en materia de ciberdefensa gracias a la nueva estrategia. Otra muestra de la estrecha colaboración con la empresa privada fue el desarrollo por parte de Microsoft de un software de código abierto llamado “ElectionGuard” para ayudar a salvaguardar las elecciones de 2020 (Parks, 2019). Con la experiencia adquirida en las elecciones anteriores, Microsoft anticipó ataques dirigidos a sistemas electorales estadounidenses, campañas políticas u ONG,s que trabajan estrechamente con tales campañas (Burt, 2019).

En octubre de 2020, los medios de comunicación publicaron que el USCYBERCOM llevó a cabo operaciones para desarticular una botnet[5] maliciosa conocida como “TrickBot” como parte de sus esfuerzos para proteger las elecciones presidenciales de 2020 de la interferencia rusa. Trickbot, una plataforma atribuida a actores rusos, proporcionaba importantes capacidades de reconocimiento y acceso, y se utilizaba con frecuencia para distribuir ransomware[6]. El ataque a la botnet contó con la colaboración del sector privado, de forma simultánea al ataque del USCYBERCOM, Microsoft también atacó Trickbot. El efecto combinado fue la interrupción de los servidores de mando y control de la red de bots (Chesney, 2020). El ataque se encuadraba dentro del concepto “Persistent Engagement”; es decir, la imposición de costes acumulativos a un adversario manteniéndolo constantemente comprometido.

También el gobierno Iraní intentó intervenir en las elecciones presidenciales. El 21 de octubre se enviaron correos electrónicos amenazantes a demócratas de cuatro estados (Nakashima, 2020c). El director de Inteligencia Nacional, John Ratcliffe, anunció esa noche que los correos que utilizaban una dirección de remitente falsa, habían sido enviados por Irán. Como respuesta a las injerencias iraníes, el USCYBERCOM llevó a cabo una operación ofensiva en contra de los piratas informáticos que trabajan para el Cuerpo de la Guardia Revolucionaria Islámica. La respuesta inmediata al ciberataque pudo realizarse gracias a la estrategia de ciberdefensa “Defend Forward”, que al desplegar equipos a vanguardia estaban preparados para una posible actuación de Irán. Nakasone afirmó que la NSA llevaba tiempo vigilando a los iraníes y que no les pilló desprevenidos (Nakashima, 2020a).

En definitiva, la injerencia rusa en las elecciones de 2020 fue significativamente menos grave de lo que había sido en 2016 y 2018. Los expertos sugirieron varias explicaciones posibles no excluyentes entre sí. Entre ellas, el endurecimiento de las ciberdefensas estadounidenses y la reticencia de Rusia a arriesgarse a represalias (Rosenbaum, 2020).

CONCLUSIONES

Gracias a la estrategia “Defend Forward” y a sus principios asociados: “Hunt Forward”, “Persistent Engagement”, cooperación pública-privada y la cooperación con naciones aliadas, la influencia de actores externos en las elecciones de 2020 fue mínima, en contraposición a lo ocurrido en las elecciones presidenciales de 2016. Del análisis de las elecciones de 2020 puede extraerse que la madurez de la estrategia “Defend Forward” mejoró los

resultados obtenidos en 2018. El incremento de la cooperación entre entidades gubernamentales, internacionales y privadas permitió proteger de forma más efectiva las elecciones de 2020.

El ciberespacio ofrece nuevas formas de obtener ventajas estratégicas y erosionar las fuentes nacionales de poder sin recurrir a la agresión territorial o el conflicto armado. Las singulares características del ciberespacio: interconexión global, contacto constante, dificultad de atribución y la delgada línea entre los comportamientos aceptables e inaceptables que se ignoran y alteran rutinariamente, permiten a los adversarios actuar de forma persistente a través de campañas milimétricamente calculadas para evitar el conflicto armado directo y abierto, permaneciendo por debajo del umbral del uso de la fuerza, generando así incertidumbre, retraso en la toma de decisiones e inacción.

Del estudio de los casos puede deducirse que el empleo de una estrategia de ciberdefensa proactiva fue fundamental para que EE.UU pudiera conseguir y mantener la libertad de acción en el ciberespacio, proteger sus procesos electorales de 2018 y 2020, y competir de forma continua en la zona gris del conflicto.[7]

(4309)

---

[1] La disuasión por denegación pretende desincentivar a los actores, alterando el cálculo coste-beneficio, estableciendo las condiciones que induzcan a una mayor probabilidad de fracaso, a agotar sus recursos o su paciencia.

[2] La IRA se considera una granja de trolls vinculada al Kremlin. Una granja de troles es una empresa que gestiona miles de usuarios falsos. El gran volumen de cuentas falsas les permiten disponer de una masa crítica suficiente como para modificar el discurso público, y con ello, la opinión.

[3] En el RSG participaban los departamentos de Seguridad Nacional, Estado y Justicia, así como el FBI. Estaba compuesto por entre 75 y 80 personas de USCYBERCOM y la NSA (DoD).

[4] Las operaciones Hunt Forward (HFO) son operaciones estrictamente defensivas, los equipos despliegan en países amigos para observar y detectar actividades maliciosas en las redes del país anfitrión. Las operaciones generan información que refuerza la defensa nacional y aumenta la resiliencia de las redes frente a las ciber amenazas.

[5] Una botnet o red zombi es un grupo de ordenadores o dispositivos que están bajo el control de un atacante, y que se usan para perpetrar actividades malintencionadas contra una víctima.

[6] El ransomware es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta.

BIBLIOGRAFÍA

Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command. (2018). United States Cyber Command, 23 de marzo. Disponible en: https://s3.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf [Consulta 21-04-2023]

Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations. Edition A Version 1 (2020). NATO Standarization Office, 3 de febrero. Disponible en: https://www.coemed.org/files/stanags/01_AJP/AJP-3.2_EDB_V1_E_2288.pdf [Consulta: 21-04-2023]

Barnes, J. (2018b) “U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections”. *The New York Times*, 23 de octubre. Disponible en: https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html [Consulta: 21-04-2023]

Burt, T. (2019) "New cyberthreats require new ways to protect democracy". *Microsoft on the issues*, 17 de julio. Disponible en: https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/ [Consulta: 21-04-2023]

Chesney, R. (2020) “Persistently Engaging TrickBot: USCYBERCOM Takes on a Notorious Botnet”. Lawfare, 12 de Octubre. Disponible en: https://www.lawfareblog.com/persistently-engaging-trickbot-uscybercom-takes-notorious-botnet [Consulta 21-04-2023]

Corn, G. (2022) “Defend Forward and Persistent Engagement”. En *The United States’ Defend Forward Cyber Strategy. A comprehensive legal assessment.* Nueva York: Oxford University Press. ISBN 978–0–19–760182–2 (epub.)

Goldsmith, J. (2022) “Introduction”. En *The United States’ Defend Forward Cyber Strategy. A comprehensive legal assessment.* Nueva York: Oxford University Press. ISBN 978–0–19–760182–2 (epub.)

Intelligence Community Assessment: Foreign Threats to the 2020 US Federal Elections (2021) National Intelligence Council, 10 de marzo. Disponible en: https://www.dni.gov/files/ODNI/documents/ assessments/ICA-declass-16MAR21.pdf [Consulta: 22-04-2023]

International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World (2011) The President of the United States- White House, mayo. Disponible en: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Consulta: 22-04-2023]

Lopez Muñoz (1952). *La Libertad de Acción*. Madrid: Ejército.

Miller, G., Nakashima, E. y Entous, A. (2017). "Obama's Secret Struggle to Punish Russia for Putin's Election Assault" *The Washington Post*, 23 de junio. Disponible en: https://www.washingtonpost.com/graphics/201 7/world/national-security/obama-putin-election-hacking/?utm_term=.5ae7a8597553 [Consulta 22-004-2023] Miller et al. 2017

Nakashima E. (2019a) "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms". *The Washington. Post*, 26 de febrero. Disponible en: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html [Consulta: 21-04-2023]

Nakashima, E. (2019b) "U.S. Cyber Force Credited with Helping Stop Russia from Undermining Midterms". *The Washington Post*, 14 de febrero. Disponible en: https://www.washingtonpost.com/world/national-security/us-cyber-force-credited-with-helping-stop-russia-from-undermining-midterms/2019/02/14/ceef46ae-3086-11e9-813a-0ab2f17e305b_story.html [Consulta 21-04-2023]

Nakashima, E. (2020a) Washington Post 3 Noviembre de 2020 "U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election". *The Washington Post*, 3 de noviembre. Disponible en: https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html [Consulta 21-04-2023]

Nakashima, E. (2020b) "Cyber Command has sought to disrupt the world's largest botnet, hoping to reduce its potential impact on the election". *The Washington Post*, 9 de octubre. Disponible en: https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html [Consulta 21-04-2023]

Nakashima, E. (2020c) "U.S. government concludes Iran was behind threatening emails sent to Democrats". *The Washington Post*, 20 de octubre.

Disponible en: https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/ [Consulta 21-04-2023]

Nakasone, P. M. (2019b) “An Interview with Paul M. Nakasone “ Joint Force Quarterly, 92 (1) pp. 4-10. Disponible en: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf [Consulta: 22-04-2023]

NATO Warsaw Summit Communiqué emitido por los Jefes de Estado y de Gobierno participantes en la reunión del Consejo del Atlántico Norte celebrada en Varsovia los días 8 y 9 de julio de 2016 (2016). OTAN, 9 de julio. Disponible en: https://www.nato. int/cps/en/natohq/official_texts_133169.htm [Consulta: 21-04-2023]

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019. Boletín Oficial del Estado (BOE) número 103, de 30 de abril de 2019. Disponible en: https://www.boe.es/eli/es/o/2019/04/26/pci487 [Consulta: 25-04-2023]

Ottis, R. (2008) “Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability.” En: *Proceedings of the 8th European Conference on Information Warfare and Security.* Braga: Academic Publishing Limited, pp 177-182.

Ottis, R. y Lorents, P. (2010). “Cyberspace: Definition and Implications”. En *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton: Academic Publishing Limited, pp. 267-270.

Parks, M. (2019) "Ahead Of 2020, Microsoft Unveils Tool To Allow Voters To Track Their Ballots" *NPR*, 6 de mayo. Disponible en: https://www.npr.org/2019/05/06/720071488/ahead-of-2020-microsoft-unveils-tool-to-allow-voters-to-track-their-ballots [Consulta: 21-04-2023]

Publicación Doctrinal Conjunta PDC-01(A) Doctrina para el empleo de las Fuerzas Armadas (2018). EMAD, 27 de febrero de 2018, pp.79. Disponible en: https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html [Consulta: 21-04-2023]

Publicación Doctrinal Conjunta PDC-3.20. Doctrina de operaciones en el ámbito ciberespacial.(2021). EMAD, 28 de abril. Disponible en: http:/intra.mdef.es/portal/intradef/Ministerio_de_Defensa/CCDC/CCDC/Publicaciones/Nacional) [Consulta: 21-04-2023]

Report On The Investigation Into Russian Interference In The 2016 Presidential Election (Mueller Report). (2019) U.S. Department of Justice (Special Counsel

Robert S. Mueller, III), marzo. Disponible en: https://www.justice.gov/archives/sco/file/1373816/download [Consulta: 22-04-2023]

Riley, M., y Robertson, J. (2017) "Russian Hacks on U.S. Voting System Wider Than Previously Known". *Bloomberg*, 13 de junio. Disponible en: https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections [Consulta: 21-04-2023]

Rosenbaum, E. (2020) "Most important 2020 election misinformation threat is not coming from overseas: Facebook former security chiefAlex Stamos". *CNBC*, 30 de octubre. Disponible en: https://www.cnbc.com/2020/10/30/most-important-2020-election-misinformation-threat-not-from-overseas.html [Consulta 21-04-2023]

The Department of Defense Cyber Strategy (2015). Department of Defense (DoD), 17 de abril. Disponible en: https://www.hsdl.org/c/view?docid=764848 [Consulta: 22-04-2023]

The Fiscal Year 2021 Budget Request for US Cyber Command and Operations in Cyberspace: Hearing of Gen. Nakasone. House Committee on Armed Services, Subcommitee on Intelligence, Emerging Threats and Capabilities. Nakasone, P. M. (2020)