

Capítulo 12

Capacidades ciber en los conflictos contemporáneos*

DOI: <https://doi.org/10.25062/9786287602809.12>

Juan David Zuleta
Andrés Acosta Muñoz

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Los eventos actuales demuestran que el conflicto cibernético ya es común en todo el mundo. Este capítulo aborda las estrategias y tácticas agresivas de la guerra cibernética en todas las etapas de la planificación de la seguridad y defensa nacionales. Se concluye que el liderazgo de seguridad y defensa nacional debe mejorar drásticamente su comprensión de la tecnología, la ley, la ética y los ataques cibernéticos, para que de esta manera se pueda tener en cuenta un contexto amplio de la guerra multidominio.

Palabras clave: defensa; estrategia, guerra ciber; inteligencia; seguridad.

* Este capítulo es resultado de investigación adscrito al proyecto "*Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia*", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Juan David Zuleta

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Conducción y Administración de Unidades Militares, y Especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Armas y Servicios del Ejército Nacional. Especialista en Administración Ecuestre, Escuela de Caballería del Ejército Nacional. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: juan.zuleta@buzonejercito.mil.co

Andrés Acosta Muñoz

Coronel del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, y especialista en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Seguridad y Defensa, Universidad de Nebrija, España. Especialista en Alta Gerencia, Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0002-2813-5471> - Contacto: andres.acosta@esdeg.edu.co

Citación APA: Zuleta, J. D., & Acosta Muñoz, A. (2024). Capacidades ciber en los conflictos contemporáneos. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 287-310). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.12>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

En este capítulo se abordan los conflictos contemporáneos, en los cuales se emplean las capacidades y los avances tecnológicos del dominio ciberespacial, tanto en la ofensiva como en la defensiva, para degradar las capacidades del adversario y generar un alto grado de desestabilización en el desarrollo de acciones militares antes, durante y después de un conflicto. Además, se analiza la importante participación de las unidades de Fuerzas Especiales (FF. EE.) e Inteligencia en el desarrollo de este tipo de acciones y operaciones cibernéticas, en la medida en que se están convirtiendo en la más importante tarea de los Estados para enfrentar a sus amenazas.

Al respecto conviene decir que el mundo está cambiando a pasos agigantados y que el desarrollo de las tecnologías de la información y las comunicaciones (TIC) avanza a un ritmo tan acelerado, que de alguna manera están superando las expectativas de las capacidades estratégicas, operacionales y tácticas de las Fuerzas Armadas en todo el mundo. La implementación de nuevas tecnologías desafía los parámetros y factores de las guerras convencionales, al tiempo que transforma las estrategias que los Estados adoptan para enfrentar a sus adversarios en los entornos nacionales, vecinales, regionales, continentales, hemisféricos y globales.

Siguiendo este criterio es posible identificar cuáles son las principales potencias en la temática, como ciertamente lo son Estados Unidos, China, Rusia, Israel e Irán, en la medida en que estos países son beligerantes en el ciberespacio y destinan recursos humanos, técnicos y económicos para desarrollar sus “ciberfuerzas”. En general, se puede afirmar que lo hacen con una doble intención: en primer lugar, garantizar la seguridad y la defensa de sus ciberespacios específicos y, en segundo lugar, ejercer poder e influencia entre sus ciudadanos, aliados y potenciales

adversarios (Colom et al., 2013). En últimas, todo esto tiene el propósito de prevenir y reaccionar ante la presencia de ataques cibernéticos que puedan poner en riesgo la continuidad y la disponibilidad de los servicios críticos del país.

No obstante, esto tan solo es la punta del iceberg. En la actualidad existen diferentes ramificaciones en los lineamientos estratégicos en los niveles ofensivo y defensivo, los cuales deben ser tratados para hacer frente a los diversos riesgos y amenazas que hay en el ciberespacio. En especial cuando se trata de los escenarios bélicos contemporáneos, en los cuales se requiere la intervención de unidades de FF. EE.

Además, este capítulo busca establecer la relación que tienen los nuevos requerimientos de las guerras contemporáneas en cuanto a la implementación del arte y el diseño operacional, con la identificación del centro de gravedad de las amenazas cibernéticas usando la inteligencia estratégica. Vale la pena aclarar que estos procesos iniciales de formulación y lógica “constituyen el sistema nervioso central de la doctrina del Ejército Nacional de Colombia y responde a las necesidades que tienen los comandantes y estados mayores de resolver situaciones en ambientes operacionales volátiles, inciertos, complejos y ambiguos” (Ejército Nacional de Colombia, 2019, p. 19).

Por otra parte, se evalúan las debilidades que tiene la concepción doctrinaria sobre el empleo de la Inteligencia y las capacidades cibernéticas en los conflictos contemporáneos mediante algunos estudios de caso. Esto significa que se analiza la relación entre las Operaciones de Inteligencia realizadas por medios cibernéticos, la tasa de éxito en el cumplimiento de los objetivos y los principales retos y desafíos que conlleva emplear herramientas cibernéticas en los escenarios contemporáneos.

Finalmente, se estudia el alcance de las estrategias y las Operaciones de Inteligencia militar en los conflictos y guerras contemporáneas desde varias perspectivas del dominio ciberespacial, con la finalidad de interpretar los propósitos, las características y los resultados de su desarrollo.

Metodología

La investigación se realizó con herramientas que permiten hacer un análisis comparativo de diversas teorías y eventos relacionados, lo cual implica un ejercicio

consistente de revisión bibliográfica sobre el tema y las capacidades cibernéticas empleadas en los conflictos contemporáneos. Además, se hace una investigación documental en la que se recopiló información sobre los lineamientos estratégicos a nivel ofensivo y defensivo.

De esta manera, se pudieron obtener registros de diversas fuentes bibliográficas, por ejemplo, en revistas, artículos científicos, libros, material archivado y otros trabajos académicos, lo cual permitió construir una visión general y particular de la naturaleza de la guerra contemporánea, los retos y las oportunidades de las FF. EE. y la Inteligencia. Si bien se trata de un estudio principalmente cualitativo que hace una conceptualización, evaluativa y observacional, también con apoyo en datos cuantitativos se explican los fenómenos observados mediante la recolección de datos digitales, los cuales son analizados con métodos que se basan en técnicas matemáticas, estadísticas o informáticas.

Posteriormente, se realiza un análisis comparativo y descriptivo de cada uno de los escenarios señalados, consistente en recolectar muestras con el propósito de observar el comportamiento de las diferentes variables expuestas como problema de investigación. Finalmente, se hace un análisis del discurso a varias series de documentos, especialmente políticas públicas y doctrina militar sobre las capacidades cibernéticas, con el fin de explicar el enfoque teórico que subyace en el concepto.

Los nuevos requerimientos de la guerra contemporánea

En la guerra contemporánea se encuentran varios escenarios y acontecimientos que contribuyen a formar una idea específica de cómo están evolucionando los conflictos armados. En otras palabras, existen razones para creer que los dominios de la guerra interactúan física y virtualmente. Así lo afirma Patrikarakos (2021), quien considera que hay dos guerras, una que se batalla en los dominios físicos (terrestre, marítimo, aéreo y espacial), y otra que se desarrolla en los entornos virtuales (ataques cibernéticos, sabotaje, desinformación y otro tipo de acciones). Estos aspectos hacen considerar que se presenta una nueva dinámica en los conflictos contemporáneos y, por lo tanto, nuevas necesidades para desestabilizar al adversario en tiempos de guerra y conflicto.

En este escenario, se ha despertado el interés de los gobiernos en todo el mundo por impactar, penetrar e influir las políticas sociales y económicas mediante el uso de las TIC. Como consecuencia, están identificando parcialmente las posibilidades, los retos y los desafíos que representa el amplio mundo del ciberespacio, al tiempo que expanden las estrategias y crean organizaciones de ciberdefensa y ciberseguridad, las cuales dedican sus esfuerzos a enfrentar las amenazas ciberespaciales. Esto quiere decir que las naciones están lidiando tan solo con la superficie de la “Cuarta Revolución Industrial” (Industria Conectada 4.0), la cual se caracteriza por una mezcla vanguardista de técnicas de producción con sistemas inteligentes, que se integran con las organizaciones y las personas, pero que a su vez cuentan con vulnerabilidades que son aprovechadas para generar alteración y daño en las infraestructuras críticas de una nación específica.

Al respecto conviene decir que las especialidades y necesidades de las fuerzas de seguridad y defensa han demandado varios cambios en las instituciones, los cuales han favorecido significativamente la protección de sus infraestructuras críticas. En otras palabras, las capacidades cibernéticas se han convertido en una tendencia que cada día toma más fuerza, al punto de fusionarse simbióticamente en las especialidades diferenciadoras de cada fuerza militar, generando innovaciones en sus organizaciones y plasmando una revolución positiva en el manejo de los riesgos y las amenazas a la seguridad nacional. Según Kenneth Geers (2009), “prácticamente todo lo que sucede en el mundo real se refleja en el ciberespacio. Para los planificadores de seguridad nacional, esto incluye propaganda, espionaje, reconocimiento, objetivos y, en una medida desconocida, la guerra misma” (p. 145).

Al respecto, conviene agregar que para Geers (2009) existen cinco tácticas comunes utilizadas en la guerra cibernética: el espionaje, la propaganda, la denegación de servicios (DoS), la modificación de datos y la manipulación de la infraestructura. En este contexto, se puede asegurar que el ciberespacio es, en definitiva, el “nuevo escenario de confrontación” entre Estados, naciones, democracias, dictaduras, organizaciones criminales, terroristas, entre otros.

Por esta razón hay una competencia entre potencias y países en vía de desarrollo para crear nuevas estructuras y organizaciones facilitadoras que permitan, por un lado, proteger las capacidades informáticas propias y, por otro, ser capaces de realizar operaciones cibernéticas con diferentes objetivos, principalmente orientados a afectar las capacidades de las amenazas. Por lo tanto, en este punto se puede decir que surge la ciberguerra.

Con base en este panorama, a continuación se desarrolla la Metodología de Diseño del Ejército (MDE) para definir la estructuración de un ambiente operacional (AO) desde una perspectiva sistémica durante el proceso de operaciones, relacionado con las capacidades cibernéticas en los conflictos contemporáneos. Con este propósito se empleará una serie de diagramas de análisis de red para visualizar y describir el ambiente, lo cual permite mostrar de manera sencilla y didáctica las conexiones que existen en las diferentes redes para entender el AO en torno a los riesgos y las amenazas en el dominio ciberespacial.

Vale la pena aclarar que el AO es definido por el Ejército Nacional de Colombia (2017b) como la “composición de condiciones, circunstancias e influencias que afectan el empleo de las capacidades y que pesan en las decisiones del comandante” (p. 1-2). Desde esta perspectiva, en los siguientes apartados se enmarca el problema operacional, es decir, se presenta una situación general de los aspectos representativos en los conflictos contemporáneos, los cuales estarán relacionados con los lineamientos estratégicos a nivel ofensivo y defensivo en el dominio ciberespacial, así como con la estructura en el enfoque operacional.

Guía de Planeamiento Estratégico 2018-2022

En el *Plan Estratégico del Sector Defensa y Seguridad - Guía de Planeamiento Estratégico 2018-2022 (PES)*, el Ministerio de Defensa Nacional (MDN) emitió instrucciones a las Fuerzas Militares para direccionar “la misión constitucional de la fuerza pública y la consecución de los objetivos estratégicos nacionales” (MDN, 2018, p. 3). Además, establece la hoja de ruta de la planeación integrada del sector defensa y seguridad durante el cuatrienio, partiendo del análisis de las amenazas y los retos a la defensa y la seguridad nacionales. Específicamente, estas fueron las premisas que el MDN (2018) dio a las Fuerzas Militares:

1. Los riesgos y las amenazas al Estado en el ciberespacio representan una nueva preocupación, dado que pueden provenir de diferentes actores, de cualquier parte del mundo, y buscan cumplir objetivos asociados a diversos fenómenos, como la criminalidad, el espionaje, el sabotaje, el terrorismo, entre otros (MDN, 2018, p. 8).
2. Frente a los retos y las amenazas presentados en el ámbito externo, el *Plan Estratégico del sector Defensa y Seguridad - Guía de Planeamiento Estratégico 2018-2022 (PES)* propone la defensa de los intereses nacionales a través de una estrategia robusta que, adicionalmente, fortalezca

las capacidades en seguridad digital, ciberdefensa, inteligencia y contra inteligencia (MDN, 2018, p. 9).

Situación general

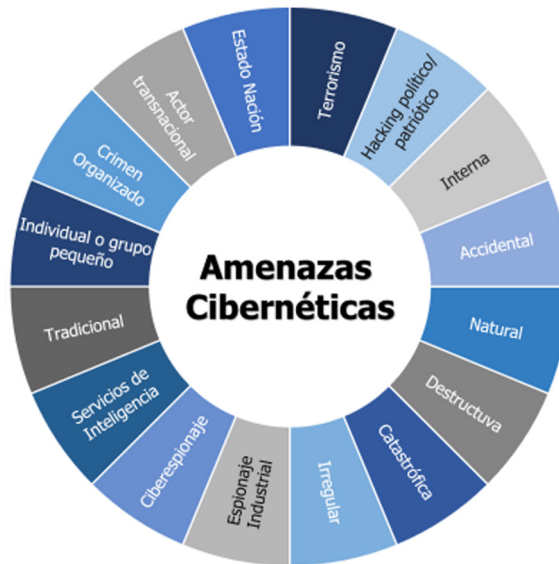
En 1962, el Departamento de Defensa de los Estados Unidos, a través de la Agencia de Investigación de Proyectos Avanzados (ARPA, por la sigla en inglés de *Advanced Research Projects Agency Network*), solicitó el desarrollo de una tecnología que permitiera la comunicación interconectada entre diferentes instituciones gubernamentales. Posteriormente, en 1969, se logró exitosamente la prueba de mensaje, con la cual se creó la primera red de comunicación entre la Universidad de Stanford y la Universidad de California en los Ángeles (UCLA).

Después, en el año de 1988, hizo su aparición el primer código o software malicioso del mundo, el cual fue denominado con el nombre de *Worm Morris* ('Gusano Morris'). Al ser el primero en su especie, generó estragos en las redes computacionales y en los ordenadores de la época. Contaba con la capacidad de autorreplicarse rápidamente, de manera que logró una afectación directa al internet. El impacto que generó en los sistemas informáticos permitió evidenciar las vulnerabilidades de la internet. Todo esto exigió a los desarrolladores definir protocolos de seguridad que protegieran las redes informáticas de futuros ataques devastadores. Por lo tanto, los hechos ocurridos en ese año abrieron un campo de oportunidades para crear una variedad inimaginable de malwares, lo cual cambió significativamente las posibilidades de interacción de los sistemas informáticos. De esta manera surgieron los ciberataques y el ciberespionaje.

En 1990, el Consejo Europeo para la Investigación Nuclear (CERN, por la sigla en francés de *Centre Européen de Recherche Nucléaire*), junto con varios físicos ubicados en Ginebra y Suiza, desarrollaron el lenguaje HTML (lenguaje de marcado hipertextual) y el mismo año también se creó el primer cliente web o la World Wide Web (WWW).

Ahora bien, en la década actual (2020-2030) existen diversos agentes de la amenaza del dominio ciberespacial (figura 1), los cuales tienen diferentes tipos o múltiples finalidades, como motivos económicos, políticos, intelectuales, inteligencia, espionaje industrial, entre otros. Aún así, el riesgo más grande proviene de los Estados y las organizaciones de inteligencia, que, mediante la manipulación de estructuras o grupos de diferente índole, ejecutan sus actividades en busca de cumplir objetivos específicos.

Figura 1. Amenazas cibernéticas.



Fuente: Elaboración propia.

Las amenazas más recurrentes en el ciberespacio se pueden catalogar de acuerdo con las siguientes denominaciones: amenaza Estado-nación; amenaza actor transnacional; amenaza crimen organizado; amenaza individual o de grupos pequeños; amenaza tradicional; servicios de inteligencia; ciberspionaje; espionaje industrial; amenaza irregular; amenaza catastrófica; amenaza destructiva; amenaza natural; amenaza accidental; amenaza interna; *hacking* político/patriótico y terrorismo.

Estructura del ambiente operacional

La nueva tipología de batalla está enmarcada en la posguerra fría, en la cual se planteó la empleabilidad de los computadores y las comunicaciones en la red para enfrentar las amenazas mediante el desarrollo y la ejecución de información con propósitos psicológicos y de desarticulación logística. Asimismo, se caracteriza por emplear tecnologías de la información en diferentes organizaciones de nivel estratégico, operacional y táctico, los cuales tienen una infinidad de componentes y recursos de las fuerzas armadas a nivel global.

En los Estados Unidos, que prácticamente son considerados la cuna del internet, varios pensadores, militares, políticos, etc., están invirtiendo tiempo y recursos para analizar la fenomenología de los riesgos y las amenazas cibernéticas, así

como las alternativas que les sean necesarias para logran mantener el liderazgo frente al entorno global del dominio ciberespacial.

Por su parte, la Organización del Tratado del Atlántico Norte (OTAN) define que la infraestructura crítica de un país está compuesta por instituciones públicas y privadas de los sectores de la agricultura, los alimentos, el agua, la salud pública, los servicios de emergencia, el gobierno, la industria de defensa, la información y las telecomunicaciones, la energía, el transporte, la banca y las finanzas, los productos químicos y materiales peligrosos y la administración postal (Geers, 2009).

Además, se considera que el ciberespacio es el sistema nervioso, el sistema de control de un país. El ciberespacio está formado por cientos de miles de ordenadores interconectados, servidores, enrutadores, concentradores y cables de fibra óptica que permiten fusionar la infraestructura crítica. Por esta razón, el funcionamiento saludable del ciberespacio es esencial para la economía y la seguridad nacionales.

Identificación del problema y el desarrollo de opciones

Las razones estratégicas por las cuales la guerra cibernética está en aumento se relacionan con varios factores preponderantes. En primer lugar, la internet es vulnerable a los ataques cibernéticos. Indiscutiblemente no existe seguridad que garantice al cien por ciento su invulnerabilidad. Por lo tanto, en la actualidad se puede afirmar que no existe un sistema totalmente seguro en el mundo, el cual sea capaz de evitar los diferentes tipos de ataque cibernéticos. Además, el diseño imperfecto de internet permite a los hackers leer, eliminar y/o modificar subrepticamente la información almacenada o enviada entre computadores. Por lo tanto, los ataques, armados con código malicioso en constante evolución, probablemente tengan más rutas de acceso a su red y los secretos que contiene de las que los administradores del sistema pueden proteger.

En segundo lugar, se encuentra el alto retorno de la inversión. Los objetivos de los practicantes de la guerra cibernética hablan por sí mismos: el robo de datos de investigación y desarrollo, el espionaje de comunicaciones sensibles y la entrega de propaganda. Lo distintivo de la piratería informática radica en el hecho de que se puede intentar por una fracción del costo y el riesgo de cualquier otra estrategia de recopilación o manipulación de información.

En tercer lugar, la insuficiencia de la ciberdefensa. La defensa cibernética sigue siendo una disciplina inmadura, aunque en constante evolución. Las habilidades tradicionales de aplicación de la ley son inadecuadas, y es difícil retener al personal

con habilidades altamente comercializables. Las investigaciones informáticas desafiantes se complican aún más por la naturaleza internacional de internet. Finalmente, no existen operaciones ofensivas en el ciberespacio patrocinadas por los Estados ni cooperación entre las fuerzas del orden.

En cuarto lugar, se encuentra la negación plausible. La arquitectura laberíntica de internet ofrece a los ciberatacantes un alto grado de anonimato. Los hackers inteligentes pueden enrutar ataques a través de países con los que el gobierno de la víctima tiene malas relaciones diplomáticas y no coopera con las fuerzas del orden. Incluso las investigaciones exitosas a menudo conducen solo a otra computadora pirateada. Los gobiernos de hoy se enfrentan a la perspectiva de perder un conflicto cibernético sin conocer nunca la identidad de su adversario.

Por último, y en quinto lugar, se encuentra la participación de agentes no estatales. Los Estados-nación se esfuerzan por mantener tanto control como puedan sobre los conflictos internacionales, pero la globalización y la internet han fortalecido considerablemente la capacidad de cualquier persona para seguir los acontecimientos actuales, así como el poder para darles forma. Las subculturas transnacionales ahora se fusionan espontáneamente en línea e influyen en innumerables agendas políticas, sin informar a ninguna cadena de mando. En este sentido, un desafío para el liderazgo de la seguridad nacional es que esta actividad podría poner a la delicada diplomacia fuera de control.

Estos fenómenos parecen confirmar que todos los conflictos políticos y militares tienen una dimensión cibernética, cuyo tamaño e impacto son difíciles de predecir, pues los atacantes tienen a su disposición una amplia variedad de estrategias y tácticas efectivas de guerra cibernética.

Por lo tanto, internet es vulnerable a los ataques de naturaleza cibernética. Además, su poder amplificador significa que las futuras victorias en el ciberespacio podrían traducirse en victorias sobre el terreno. Tanto los actores estatales como los no estatales disfrutan de un alto retorno de la inversión en tácticas cibernéticas, que van desde la colocación de propaganda cuidadosamente elaborada hasta la manipulación de la infraestructura crítica del adversario.

Las debilidades en la concepción doctrinaria

La concepción doctrinaria de las fuerzas militares a nivel mundial referente a este tipo de temas se encuentra en etapas muy tempranas, así que existe un largo camino por recorrer para comprender y establecer normativas que permitan

implementar estrategias, métodos, procedimientos y tácticas para enfrentar los riesgos y las amenazas en el ciberespacio. Como consecuencia, es necesario establecer algunos factores importantes para desarrollar una aproximación doctrinaria que permita enfrentar estos desafíos. A continuación, se identifica su empleo en la Inteligencia, las capacidades cibernéticas en los conflictos contemporáneos y estudios de caso que permiten caracterizar algunos aspectos que se deben tener en cuenta en este tipo de iniciativas.

Empleo de la Inteligencia

Sin lugar a duda, las capacidades que brindan las herramientas de la guerra cibernética para los estamentos de seguridad y defensa en el campo de la inteligencia son excepcionales. Por lo tanto, es posible asegurar que estas capacidades siguen siendo una gran posibilidad para lograr una ventaja estratégica con respecto a los adversarios. La infiltración, penetración y captación de información son sus principales ventajas, pues garantizan las puertas de acceso furtivas necesarias para alcanzar con éxito las Operaciones de Inteligencia.

Capacidades ciber en conflictos contemporáneos

Según Patrikarakos (2021), “los términos como guerra híbrida, desinformación y granja de *trolls*, se han convertido en palabras de moda en nuestra era de la pos-verdad” (p. 14). Sumado a esto, actualmente la probabilidad de controlar la internet, el tráfico, los móviles, los sistemas de seguridad, etc., no es un cuento de ciencia ficción, sino, más bien, parte del concepto general de la ciberguerra. Por esta razón, “los estrategas deben ser conscientes de que parte de todo conflicto político y militar tendrá lugar en internet” (Geers, 2009, p. 58).

Los ataques cibernéticos han mejorado e incrementado su capacidad y complejidad; año tras año un nuevo virus, troyano o software malicioso aparece en escena. Habilidades características para interrumpir procesos, abrir puertas traseras, modificar códigos, facilitar el robo de información, recolectar información de las relaciones comerciales de diferentes organizaciones y degradar sistemas son la señal de que las características del ciberespacio hasta ahora están en pleno descubrimiento.

Por lo tanto, se debe reconocer que no existe ninguna aplicación de software que no tenga vulnerabilidades. En otras palabras, los sistemas industriales, comerciales, militares, gubernamentales, policiales, etc., requerirán de una mayor atención, preferiblemente, por el impacto que representa cada una de las categorías y

la manera inmediata en que pueden afectar las infraestructuras críticas. Debido a estas características, se pueden convertir en objetivos de muchas organizaciones, en especial de grupo de hackactivistas, cibercriminales, ciberterroristas, Estados, entre otros. Es importante dejar claro que los efectos de estos ataques serían devastadores para las infraestructuras críticas de cualquier nación.

Estudios de casos

A continuación, se presentan varios estudios de casos relacionados con las capacidades cibernéticas en los conflictos contemporáneos, los cuales permiten identificar, evaluar y analizar, en el entorno general del ciberespacio, los riesgos y las amenazas a las cuales se enfrentan las instituciones de seguridad y defensa nacionales.

Chechenia (1994)

En la era de internet, las noticias sin editar de un frente de guerra pueden llegar en tiempo real. Los usuarios de internet de todo el mundo desempeñan un papel importante en los conflictos internacionales al publicar información, ya sea en formato de texto o imagen, en un sitio web.

Según Thomas Timothy (2003), desde los primeros días de la World Wide Web, las fuerzas prochechenas y prorrusas han librado una guerra virtual en internet, la cual se desarrolla simultáneamente en los campos de batalla reales. El movimiento separatista checheno, en particular, es considerado un pionero en el uso de la web como una herramienta para entregar poderosos mensajes de relaciones públicas. La hábil colocación de propaganda y otros tipos de información, como el número de una cuenta de banco para recaudar fondos de guerra en Sacramento, California, ayudó a unir a la diáspora chechena.

Además, la información más efectiva, sin embargo, no era prochechena, sino antirrusa. Las imágenes digitales de cadáveres ensangrentados sirvieron para poner a la opinión pública en contra de los supuestos excesos militares rusos. En 1999, justo cuando los funcionarios del Kremlin negaban un incidente en el que un autobús checheno fue atacado y muchos pasajeros murieron, las imágenes del incidente aparecieron en la web. A medida que avanzaba la tecnología, los internautas veían videos en *streaming* referentes a la actividad militar chechena de manera favorable, como fueron las emboscadas a convoyes militares rusos (Goble, 1999).

Cabe aclarar que, según Goble (1999), el gobierno ruso admitió la necesidad de mejorar sus tácticas en el ciberespacio. En 1999, Vladimir Putin, entonces primer ministro de Rusia, declaró: “Entregamos este terreno hace algún tiempo... pero ahora estamos entrando en el juego de nuevo” (Goble, 1999, s. p.). Moscú buscó la ayuda de Occidente para cerrar el importante sitio web prochecheno kavkaz.org, y anunció “la introducción de la censura militar centralizada con respecto a la guerra en el Cáucaso norte” (s. p.).

Por lo tanto, según Bullough (2002), durante la segunda guerra chechena (1999-2000), los funcionarios rusos fueron acusados de escalar el conflicto cibernético, pirateando sitios web chechenos. El momento y la sofisticación de al menos algunos de los ataques sugirieron la participación del Estado-nación, por ejemplo kavkaz.org, que estaba alojado en los Estados Unidos. Según los informes, fue desconectado simultáneamente al asalto por parte de las fuerzas especiales rusas, quienes adelantaban una operación de rescate en el interior de un teatro de Moscú sitiado por terroristas chechenos.

Kosovo (1999)

En los conflictos globalizados de la era de internet, cualquier persona con una computadora y una conexión a internet es un combatiente potencial. El primer gran compromiso militar de la OTAN siguió al crecimiento explosivo de la web durante la década de 1990. Así como Vietnam fue la primera guerra televisada del mundo, Kosovo fue su primera guerra de internet a gran escala.

Según Geers (2020), a medida que los aviones de la OTAN comenzaron a bombardear Serbia, numerosos grupos de hackers proserbios (o antioccidentales), como la Mano Negra, comenzaron a atacar la infraestructura de internet de la OTAN. Se desconoce si alguno de los hackers trabajó directamente para el ejército yugoslavo; en cualquier caso, su objetivo declarado era interrumpir las operaciones militares de la OTAN.

La Mano Negra, que tomó prestado su nombre de la sociedad secreta paneslava que ayudó a iniciar la Primera Guerra Mundial, afirmó que podían enumerar las computadoras “más importantes” de la OTAN, y que, a través de la piratería, intentaría “eliminar los datos” que contenían. El grupo adjudicó su éxito en al menos algunos puntos vulnerables, por lo menos en computadores de la Marina estadounidense, y declaró que posteriormente fue sacado de línea.

Los computadores de la OTAN, los Estados Unidos y el Reino Unido fueron atacados durante la guerra a través de la denegación de servicio y el correo electrónico

infectado por virus (se detectaron veinticinco cepas diferentes de virus) (Geers, 2020). En los Estados Unidos, el sitio web de la Casa Blanca fue desfigurado y se inició una investigación por parte del Servicio Secreto. En este escenario, mientras que los Estados Unidos afirmaban no haber sufrido “ningún impacto” en el esfuerzo de guerra general, el Reino Unido admitió haber perdido al menos parte de la información de la base de datos.

En el cuartel general de la OTAN en Bélgica, los ataques se convirtieron en una victoria propagandística para los hackers. El sitio web de asuntos públicos de la OTAN para la guerra en Kosovo, donde el organismo trató de retratar su lado del conflicto a través de sesiones informativas y actualizaciones de noticias, fue virtualmente inoperante durante varios días. El portavoz de la OTAN, Jamie Shea, culpó de la “saturación de la línea” a los “hackers en Belgrado”. Una avalancha simultánea de correo electrónico ahogó con éxito el servidor de correo electrónico de la OTAN. A medida que la organización se esforzaba por actualizar casi todos sus servidores informáticos, los ataques a la red, que inicialmente comenzaron en Belgrado, se expandieron por todo el mundo.

Oriente Medio (2000)

Durante la Guerra Fría, el Oriente Medio sirvió a menudo como campo de pruebas para armas y tácticas militares. En la era de internet se ha hecho lo mismo con la guerra cibernética.

En octubre de 2000, tras el secuestro de tres soldados israelíes, se plantaron banderas azules y blancas y un archivo de sonido que reproducía el himno nacional israelí en un sitio web pirateado de Hezbolá. Los ataques proisraelíes posteriores se dirigieron a los sitios web oficiales de organizaciones militares y políticas percibidas como hostiles a Israel, incluyendo la Autoridad Nacional Palestina, Hamas e Irán (Preatoni, 2014).

Las represalias de los hackers propalestinos fueron rápidas y mucho más diversas en su alcance. La política, el ejército, las telecomunicaciones, los medios de comunicación y las universidades israelíes se vieron afectados. Los atacantes también ejecutaron acciones en contra de sitios de valor económico puro, incluido el Banco de Israel, sitios de comercio electrónico y la Bolsa de Valores de Tel Aviv. En ese momento, Israel estaba más conectado a internet que todos sus vecinos combinados, por lo que no había escasez de objetivos. El dominio “.il” proporcionó una lista bien definida que los hackers propalestinos trabajaron metódicamente.

Como se observa, las guerras a menudo muestran nuevas herramientas y tácticas. Específicamente, durante este conflicto el programa DoS "Defender" fue utilizado con gran efecto por ambas partes, demostrando en parte que el software se puede desestabilizar más rápidamente que un tanque o un rifle. La innovación de defensa fue revisar continuamente la fecha y hora de sus solicitudes web simuladas, lo cual sirvió para derrotar los mecanismos de seguridad de almacenamiento en caché web de la época (Geers, 2004).

Por lo tanto, la guerra cibernética de Oriente Medio demostró que el portal de la era internet y los conflictos políticos pueden internacionalizarse rápidamente. Por ejemplo, según BBC News (2000), Pakistán "Hackers Club" penetró en el lobby proisraelí con sede en Estados Unidos (AIPAC, por la sigla en inglés de American Israel Public Affairs Committee), y publicó correos electrónicos confidenciales, números de tarjetas de crédito e información de contacto de algunos de sus miembros. Asimismo, Barnaby Page (2000) afirmó que "la firma de telecomunicaciones AT&T fue blanco de ataques por proporcionar apoyo técnico al gobierno israelí durante la crisis" (s. p.).

Además, Rebecca Anna Stoil y James Goldstein (2006) aseguraron que la guerra cibernética de Oriente Medio ha continuado generalmente en el ciberespacio y no se ha detenido hasta la fecha. En 2006, a medida que aumentaban las tensiones entre Israel y Gaza, los piratas informáticos propalestinos cerraron alrededor de setecientos dominios de internet israelíes, incluidos los de Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel y McDonalds Israel.

Estados Unidos y China (2001)

El 26 de abril de 2001, el Centro Nacional de Protección de Infraestructura (NIPC, por su sigla en inglés) de la Oficina Federal de Investigaciones (FBI) publicó el aviso 01-009:

Citando eventos recientes entre los Estados Unidos y la República Popular China (PRC), los hackers han intensificado sus ataques dañando páginas web. Esta actividad busca dañar a la red, y a los administradores de servicios sensibles. Allí es donde hay una mayor actividad de piratas informáticos dirigidos a Estados Unidos y sus sistemas más sensibles [...]. Los hackers chinos discutieron públicamente el aumento de su actividad durante este período, que coincide con fechas históricas importantes en la República Popular China. (Information Warfare Site [IWS], 2001, p. 86; traducción propia)

Las tensiones habían aumentado considerablemente entre los dos países después de que Estados Unidos bombardeara la embajada china en Belgrado en 1999, y después de la colisión en el aire de un avión de la Armada estadounidense y un avión de combate chino sobre el Mar del Sur de China en 2001, seguido de la detención prolongada de la tripulación estadounidense en la República Popular China.

Según Jeremy Wagstaff (2001), reportero del *The Wall Street Journal*, los hackers de ambos lados del Pacífico, como China Eagle Alliance y PoizonB0x, comenzaron la desfiguración de sitios web a gran escala y construyeron portales de hackers con títulos como "USA Kill" y "China Killer". Cuando terminaron las escaramuzas cibernéticas, ambas partes reclamaron difamaciones y DoS en infinidad de oportunidades.

En este contexto, el FBI investigó un hackeo de 17 días a una red de prueba de la red de energía eléctrica de California que comenzó el 25 de abril (Weisman, 2001). El caso fue ampliamente desestimado como exageración de los medios en ese momento, pero la CIA informó a los líderes de la industria en 2007 que no solo es posible una amenaza tangible de piratas informáticos para tal infraestructura crítica, sino que, de hecho, ya había sucedido (Nakashima & Mufson, 2008).

Estonia (2007)

El 26 de abril de 2007, el gobierno estonio trasladó un monumento soviético de la Segunda Guerra Mundial fuera del centro de su capital, Tallin, en un movimiento que inflamó la opinión pública tanto en Rusia como entre la población minoritaria rusa de Estonia.

A partir del 27 de abril, el gobierno de Estonia, las fuerzas del orden, la banca, los medios y la infraestructura de internet sufrieron tres semanas de ataques cibernéticos, cuyo impacto aún genera un gran interés por parte de gobiernos de todo el mundo.

Debido a que los estonios realizan más del 98 % de sus operaciones bancarias en línea, se entiende el impacto de múltiples ataques distribuidos de DoS, que cortaron todas las comunicaciones a los dos bancos más grandes del país durante hasta dos horas y lograron que los servicios internacionales prestados parcialmente no quedaran disponibles durante días.

Menos discutidos, pero probablemente de mayor consecuencia, tanto para los planificadores de seguridad nacional como para el personal de defensa de la red informática, fueron los ataques a la infraestructura de internet (enrutador) en los

ISP del gobierno estoniano, que se dice interrumpieron las comunicaciones del gobierno durante al menos un período de tiempo “corto”.

En el frente de la propaganda, un hacker desfiguró el sitio web del partido político del primer ministro estonio el 27 de abril, cambiando el texto de la página a una supuesta disculpa fabricada por el gobierno por haber movido la estatua, junto con la promesa de volver a su original ubicación.

Hubo un gran interés diplomático en este ataque cibernético debido en parte a la posible reinterpretación del artículo 5.º de la OTAN, según el cual “un ataque armado contra un [miembro de la Alianza] [...] se considerará un ataque contra todos ellos” (OTAN, 1949, art. 5.º). Cabe señalar que el artículo 5.º solo se ha invocado una vez, luego de los ataques terroristas del 11 de septiembre de 2001. Potencialmente, algún día podría interpretarse que abarca también los ataques cibernéticos.

Irán (2010)

Uno de los casos más representativos en la era de la guerra cibernética es el de Irán. Sin lugar a duda el desarrollo del gusano Stuxnet se convirtió en la herramienta capaz de afectar gravemente la infraestructura crítica de esta nación. Específicamente, este ataque tenía el objetivo de interrumpir las actividades nucleares que se llevaban a cabo en el reactor de Bushehr. Aquí vale la pena decir que el objetivo se cumplió satisfactoriamente, pues se logró generar un significativo retraso en el programa nuclear iraní.

Las características especiales de este caso dan cuenta de que toda su ejecución cumple las condiciones perfectas de una ciberguerra. Por esta razón, se podría inferir que la creación de esta ciberarma es en definitiva una herramienta que logró afectar los intereses nacionales de Irán. Además, establecer una operación de infiltración y de engaño para activarla y afectar las redes informáticas de un país y dejarlo vulnerables frente a ataques de cualquier naturaleza (Porteus, 2010), solo puede ser catalogado como ingenioso e innovador.

Ucrania (2014)

Ucrania fue el laboratorio de nuevos tipos de operaciones de información (Patrikarakos, 2021). El 21 de noviembre de 2013, Mustafá Nayyem, un periodista ucraniano de ascendencia afgana, escribió una publicación en Facebook instando a la gente a reunirse en Maidan Nezalezhnosti (Plaza de la Independencia) de Kiev. Quería protestar contra la decisión del presidente Viktor Yanukovich de dar marcha

atrás en su compromiso de firmar un acuerdo de asociación con la Unión Europea que habría fortalecido sus lazos políticos y económicos.

En el aniversario de esta guerra cibernética, mientras las empresas se preparaban para otra ronda de piratería, se dice que el gobierno chino pidió con éxito una retirada en el último minuto, lo que sugiere que los piratas informáticos chinos pueden compartir un mayor grado de coordinación que sus contrapartes estadounidenses (Hess, 2002).

Alcances operacionales y estratégicos de la Inteligencia militar

Internet está cambiando gran parte de la vida tal como la conocemos, para incluir la naturaleza y la conducción de la guerra. A veces, las herramientas y tácticas cibernéticas favorecerán a las naciones robustas en tecnología de la información, pero internet es una herramienta prodigiosa, que puede ser aprovechada por un grupo menor o débil para atacar a un enemigo convencional más fuerte. Al igual que con el terrorismo y las armas de destrucción masiva, la naturaleza dinámica, asimétrica y aún en evolución de los ataques cibernéticos hace que todos los aspectos de la defensa cibernética, incluida la detección, el análisis, la investigación, el enjuiciamiento, las represalias y más, sean cuestionados por los planificadores de la seguridad y la defensa nacionales.

Ahora bien, como se ha observado en los estudios de caso, es más que evidente el hecho de que los alcances operacionales y estratégicos de la Inteligencia militar se puedan beneficiar significativamente mediante el uso de herramientas cibernéticas para cumplir los objetivos planteados. No cabe la menor duda de que su potencial debe ser explorado desde una perspectiva de seguridad y defensa nacionales, ajustado a las leyes nacionales e internacionales.

Por lo tanto, analizar, diseñar, desarrollar, probar y utilizar armas cibernéticas en el futuro próximo son acciones que determinan el nuevo paso de la evolución de la guerra en el ciberespacio. Se debe agregar que los niveles estratégicos y operacionales de la Inteligencia militar deberán trabajar de la mano para proveer los recursos, métodos, técnicas, tácticas y procedimientos para el cumplimiento de las misiones de inteligencia del futuro.

Con todo y lo anterior, no se debe olvidar que los escenarios contemporáneos de la guerra tienen límites y zonas grises que deben ser tenidos en cuenta.

Escenarios contemporáneos de guerra

Patrikarakos (2021) afirma que el conflicto se aborda con dos principios rectores: en primer lugar, que la fuerza no es necesariamente el modo más apropiado para lograr los objetivos estratégicos y, en segundo lugar, que los paradigmas geopolíticos y de seguridad del siglo XX son inadecuados para dar cuenta de las amenazas contemporáneas. Por esta razón, la utilización del ciberespacio como un nuevo escenario o campo de batalla determina en muchos aspectos el efecto diferenciador en el cual los objetivos se deben alcanzar.

Al llegar a este punto, cabe indicar que existen muchas razones para determinar que los escenarios contemporáneos de la guerra están supeditados a los dominios de la guerra. La esfera del conocimiento, la influencia o actividad, el territorio sobre el cual se ejerce el dominio se convierten en unas herramientas útiles que ayudan a la descripción de áreas generales de comprensión y a la visualización y caracterización del ambiente en el que suceden las operaciones (Ejército Nacional de Colombia, 2017b).

Por lo tanto, y teniendo en cuenta que “el ciberespacio es un dominio global dentro del ambiente de la información consistente en redes interdependientes de infraestructura de tecnologías de la información y datos contenidos que incluyen: internet, telecomunicaciones, redes, sistemas informáticos y procesadores y controladores integrados” (Ejército Nacional de Colombia, 2017b, p. 491), cabe resaltar su importancia en los conflictos modernos y, por lo tanto, debe ser explotado a su máxima capacidad para generar una ventaja estratégica contra el adversario.

Conflictos de zona gris

Las leyes nacionales e internacionales no les permiten actuar de forma irracional o ilegal a las instituciones de seguridad y defensa, por lo tanto estas zonas grises son aprovechadas significativamente por las amenazas. Es decir que los lugares, áreas y actividades ilícitas que se llevan a cabo cuentan con varios respaldos importantes, entre ellos la clandestinidad, la encriptabilidad, el refugio geográfico y los vacíos de la ley.

Al respecto conviene decir que la clandestinidad permite a los actores considerados como amenazas desarrollar acciones sin determinar quiénes son y, en algunos casos, tampoco se logra saber por qué ejecutan sus planes. Además, se encuentra la encriptabilidad, la cual perfecciona a la primera debido a que dificulta la identificación forense de la red criminal. Por su parte, el refugio geográfico favorece los actos criminales de los cibercriminales, en la medida en que cuentan con

la protección de otros Estados. Finalmente, los vacíos en la ley son la base principal de la ciberseguridad y la ciberdefensa, lo cual significa que si no se cuenta con las herramientas suficientes, no se podrá generar una respuesta significativa en contra de las amenazas.

Conclusiones

Los estrategas deben ser conscientes de que parte de todo conflicto político y militar tendrá lugar en internet, cuyas características ubicuas e impredecibles hacen que las batallas que allí se libran puedan ser tan importante, si no más, que los acontecimientos que tienen lugar sobre el campo de batalla real.

Los estudio de caso sugieren que ya no se trata de tan solo piratas informáticos que tomaron por sorpresa a los planificadores de seguridad y defensa nacionales, sino que son estructuras, organizaciones y Estados mucho más complejos que deben ser estudiados desde una perspectiva más amplia.

La dinámica de la guerra contemporánea cambió gracias al dominio ciberespacial, por lo tanto, la nación que no se comprometa, hoy por hoy, en fortalecer sus medidas de ciberseguridad y ciberdefensa está caminando en una cuerda floja, literalmente, sujeta parcialmente por los dominios terrestres, marítimos, aéreos y espaciales. Es decir, no serían competidores adecuados para enfrentar las amenazas cibernéticas.

Además, la ubicuidad de los riesgos y las amenazas en el ciberespacio hacen necesario activar la ciberinteligencia en los niveles estratégicos, operacionales y tácticos, de manera que representen el camino a la categorización, la catalogación y la identificación plena de los adversarios en la guerra cibernética.

Nada puede impedir que las naciones o Estados desarrollen capacidades cibernéticas funcionales, pero el ingenio, la pericia y el conocimiento son fundamentales para conseguir el éxito en las operaciones en el ciberespacio. Asimismo, conocer la situación general, la estructura del ambiente operacional y la identificación del problema permite construir opciones en el arte operacional que favorezcan la mejor toma de decisiones en el campo de batalla.

Referencias

- BBC. (2000, 3 de noviembre). Israel Lobby Group Hakend. <https://tinyurl.com/muukxy4p>
- Bullough, O. (2002, 14 de noviembre). Russians wage cyber war on Chechen websites. <https://tinyurl.com/44h6c2vt>
- Colom, P., Coz, J., Fojón, E., & Hernández, A. (2013). Las cibercélulas: Una capacidad para la ciberseguridad y la ciberdefensa nacionales. *ARI*, (26), 1-10. <https://tinyurl.com/2p-8puuvv>
- Ejército Nacional de Colombia. (2017a). *Manual Fundamental de Referencia del Ejército MFRE 1-01 Doctrina [Público]*. Imprenta Ejército. <https://tinyurl.com/2vpdpwpm>
- Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones [Público]*. Imprenta Ejército. <https://tinyurl.com/duc7tje>
- Ejército Nacional de Colombia. (2019). *Manual de Técnicas del Ejército MTE 5-01 Metodología de Diseño del Ejército [Público]*. Imprenta Ejército. <https://tinyurl.com/3zjfspr2>
- Geers, K. (2004, 4 de abril). Cyber Jihad and the globalization of warfare: Computer networks as a battle ground in the Middle East and beyond [Presentación en diapositivas]. <https://tinyurl.com/yjabbbox>
- Geers, K. (2009). Cyberspace and the changing nature of warfare [Keynote Speech IST-076/RSY-017]. OTAN. <https://tinyurl.com/bddy3pa>
- Geers, K. (2020). #Cyberwar: International Conflict in Cyberspace. En *Alliance Power for Cybersecurity* (pp. 3-5). Atlantic Council. <https://tinyurl.com/y5p2pajx>
- Goble, P. (1999, 9 de octubre). Russia: Analysis from Washington – A real battle on the virtual front. <https://tinyurl.com/5f798nju>
- Hess, P. (2002, 29 de octubre). China prevented repeat cyber-attack on US. <https://tinyurl.com/435u3bwz>
- Information Warfare Site [IWS]. (2001). The Information Warfare Site. <https://tinyurl.com/yyczbxu2>
- Ministerio de Defensa Nacional. (2018). *Plan Estratégico del Sector Defensa y Seguridad. Guía de Planeamiento Estratégico 2018-2022*. Ministerio de Defensa Nacional. <https://tinyurl.com/2sh6v5mt>
- Nakashima, E., & Mufson, S. (2008, 19 de enero). Hackers have attacked foreign utilities, CIA analyst says. *Washington Post*. <https://tinyurl.com/43nc2fbm>
- Organización del Tratado del Atlántico Norte [OTAN]. (1949, 4 de abril). The North Atlantic Treaty. <https://tinyurl.com/yc2ujn2t>
- Page, B. (2000, 11 de noviembre). Pro-Palestinian Hackers Threaten AT&T. *TechWeb News*. <https://tinyurl.com/5n7wnenj>
- Patrikarakos, D. (2021). *Un muy moderno “niebla de guerra”, Ucrania: siete años después*. CHARCR.

- Porteus, H. (2010, 10 de junio). *The Stuxnet Worm: ¿Just another computer attack or a game changer?* [In Brief, n.º 2010-81-E]. Parliament Information and Research Service of Canada. <https://tinyurl.com/2hu9uasw>
- Preatoni, R. (2014, 10 de agosto). Calling All Hackers. <https://tinyurl.com/29w58ryh>
- Timothy, T. (2003). Information warfare in the seconds (1999-) Chechen War: Motivator for military reform? En A. C. Aldis & R. N. McDermott (Eds.), *Russian military reform 1992-2002*. Routledge.
- Wagstaff, J. (2001, 30 de abril). The internet could be the site of the next China-US Stand-off. *The Wall Street Journal*. <https://tinyurl.com/yuk6r3j2>
- Weisman, R. (2001). California power grid hack underscores threat to U. S. news factor. <https://tinyurl.com/f7nyz54y>