INSTITUTO DE INVESTIGACIONES ESTRATÉGICAS DE LA ARMADA DE MÉXICO

DA 22/18
03/04/18

Maestro
Abraham Karim González Loyola[1]

El ciberespacio en la guerra moderna

RESUMEN

El fenómeno de la guerra ha evolucionado de la mano de la tecnología de cada época. Hoy en día, las tecnologías de la información han permitido el auge de un nuevo dominio del conflicto militar: el ciberespacio. A diferencia de la tierra, aire, mar, o espacio exterior, el ciberespacio vive en un "mundo digital" que se suele creer no tiene impacto en el mundo físico en que vivimos. Sin embargo, fenómenos cibernéticos, como la ciber-cinética, han demostrado su capacidad para utilizar código de computadora – un ente digital – para provocar efectos cinéticos – en el mundo físico o "real".

Este fenómeno abre entonces una Caja de Pandora que introduce dinámicas que no eran posibles anteriormente y que modifican tanto el concepto como algunas prácticas tradicionales de la guerra. Vivimos en un mundo que día con día busca cada vez estar más interconectado entre sí a través de sistemas de computadoras, redes e Internet. Por lo tanto, cualquier individuo, grupo o nación que busque salvaguardar su seguridad o defensa y optimizar sus métodos para perseguir agendas políticas e intereses, encontrará en el ciberespacio una herramienta con el potencial de redefinir el conflicto armado humano como lo conocemos hoy en día para hacerlo.

Palabras clave: ciberespacio, ciber-cinética, guerra, guerra moderna, ataques cibernéticos, ciberguerra, ciberseguridad, hacker.

ABSTRACT

The phenomenon of war has evolved hand by hand with the technology of its time. Nowadays, information technology has given rise to a new domain of war: cyberspace. Unlike land, air, sea, or space, cyberspace lives in a "digital world" which is believed not to have any impact whatsoever in the physical world we live in.

[1] Es Licenciado en Historia por la Universidad de Maryland, Estados Unidos, graduado con honores *Summa Cum Laude;* Maestría en Estudios de Guerra por King's College London, Londres, Reino Unido. Es catedrático de la Universidad Anáhuac México, Campus Norte, CDMX, México e Investigador Externo del Instituto de Investigaciones Estratégicas de la Armada de México.

However, cybernetic phenomena, such as kinetic cyber, have demonstrated their ability to utilise computer code – a digital entity – to create kinetic effects – in the physical or "real" world.

This phenomenon then opens a Pandora's Box that introduces dynamics that were not possible before and which modify both the concept as well as some traditional practices of warfare. We live in a world that day by day seeks to become more interconnected through computer systems, networks and the Internet. Therefore, any individual, group or nation who seeks to safe keep its security or defence as well as to optimise its methods for pursuing political agendas and interests, will find in cyberspace a tool with the potential to redefine human armed conflict as we know it today to do so.

Key words: cyberspace, kinetic cyber, war, modern warfare, cyberattacks, cyberwar, cybersecurity, hacker.

INTRODUCCIÓN

Vivimos en tiempos interesantes para el estudio de la guerra y la estrategia militar. Los últimos 100 años han visto un desarrollo sin precedentes en los dominios en que se desenvuelven los conflictos militares.

Si observamos la evolución del conflicto militar desde la primera batalla sobre la que tenemos información detallada - librada en Megiddo, hoy Israel, hace aproximadamente 3,500 años - nos daremos cuenta que, durante 3,400 de esos años, la guerra se libró exclusivamente en los dominios terrestres y marítimos.

No fue sino hasta principios del siglo XX que un nuevo dominio entró al conflicto militar: el aire. Ya para tiempos de la Primera Guerra Mundial se vieron las primeras operaciones aéreas, principalmente en misiones de reconocimiento, pero también algunos bombardeos y combates aéreos en menor escala. Para finales de la Primera Guerra Mundial, fue evidente que el aire se convertiría en un dominio del conflicto militar crucial y por tanto debía ser estudiado y practicado bajo los principios de la estrategia militar, así como la tierra y el mar lo habían sido durante milenios.

Tan solo unas décadas después, la Guerra Fría y la famosa "Carrera del Espacio" entre la Unión Soviética y los Estados Unidos de América (EEUU), dieron pie a la exploración de un nuevo dominio del conflicto militar: el espacio exterior. A pesar de toda la ciencia ficción que ha envuelto el conflicto espacial desde entonces, sí ha existido una pugna militar por la superioridad aeroespacial que data desde los años 60s. Proyectos como el *Almaz* de la Unión Soviética o el *Blue Gemini* de los EEUU son pioneros de los programas militares espaciales. Desde entonces, proyectos que involucran misiles balísticos, misiles interceptores, armas laser anti-satélites, e incluso bombas nucleares que liberan pulsos electromagnéticos que desactivan muchos de los satélites en órbita, han formado parte del ajedrez bélico que se juega en el espacio exterior hasta el día de hoy.

Sin embargo, los últimos años del siglo XX y la primera década del siglo XXI vieron el auge de un nuevo dominio del conflicto muy distinto a todos los que le precedieron: el ciberespacio. La peculiaridad más evidente que tiene el ciberespacio –que es considerado una sub-categoría del dominio de la información (Pollpeter, 2012, p. 194)– es que es el único de los que hoy se consideran los cinco dominios del conflicto (tierra, mar, aire, espacio e información) que aparentemente opera fuera del espacio físico o "mundo real", lo cual trae consigo características y dinámicas exclusivas e interesantes que veremos en este análisis.

Así como el ciberespacio abre oportunidades únicas que no eran posibles antes de su prominencia, genera también dudas y confusión sobre su alcance, cómo realmente funciona y bajo qué dinámicas opera dicho dominio. El verdadero lugar y rol del ciberespacio es un tema que académicos y analistas militares debaten vehementemente hoy en día. Esto indica que a pesar de los significativos avances que se han hecho en el mundo cibernético en las últimas dos décadas, es un concepto que aún está "en ciernes", pues no hay aún un consenso homogéneo entre países u organizaciones en lo que respecta al papel que juega el ciberespacio dentro de la seguridad nacional, internacional, la defensa y los conflictos armados.

Comúnmente se hace una analogía entre el estado actual de nuestro entendimiento del ciberespacio con aquél al que se enfrentaron académicos, analistas y militares a principios del siglo XX con el auge del espacio aéreo. En su momento, había quienes consideraban el espacio aéreo como una mera herramienta de inteligencia a través del reconocimiento que se pudiera obtener de él, mientras otros veían un enorme potencial con la capacidad de redefinir la práctica de la guerra (Foster, 2017).

Al final del día, los avances tecnológicos, la experimentación, la puesta en práctica de los conceptos preconcebidos a principios del siglo, y las demandas de los conflictos militares de la época fueron los elementos que determinaron el rumbo y el papel que jugaría el espacio aéreo en el conflicto militar. Hoy en día el espacio aéreo es considerado el terreno de ventaja supremo, al grado de que, fuera de las armas nucleares, el símbolo de una potencia militar es el portaviones, cuya principal función es la de proyectar poder a través de la supremacía aérea. Este proceso ha sido el resultado de una evolución del concepto del espacio aéreo a través del tiempo. Es aventurado asumir, por ejemplo, que los primeros pensadores y analistas de dicho dominio concibieran siquiera el concepto de un portaviones desde un inicio.

La anterior analogía sirve para ilustrar el proceso al que nuevos dominios del conflicto pueden ser sujetos. Es una analogía precisa pues el estado actual del ciberespacio comparte las características evolutivas por las que pasó el dominio aéreo. Por ejemplo, actualmente hay una clara división entre dos grupos, los ciber-escépticos y los ciber-alarmistas. El primer grupo lo conforman aquellos que afirman que el ciberespacio y las nuevas tecnologías de la información no harán ninguna diferencia relevante en el mundo y desechan la idea de una ciberguerra; el segundo grupo lo conforman aquellos que consideran el ciberespacio y su alcance

como una amenaza inminente que pone en alto riesgo a individuos, grupos y naciones al borde de una guerra cibernética con consecuencias devastadoras (The Economist, 2013).

Así como hay argumentos válidos de ambos bandos, la realidad es que un fenómeno tan complejo como lo es el ciberespacio, cuyo entendimiento aún está en su infancia, no puede ser visto en absolutos de blanco o negro como proponen estos grupos.

Lo que es innegable es que el proceso de evolución del dominio de la información, en particular el ciberespacio, está ya tomando lugar. Desafortunadamente, dicha evolución está sucediendo más rápido de lo que analistas, académicos y ciber-expertos logran definirla y encajarla en el enorme rompecabezas que es el ciberespacio, el dominio de la información, la seguridad nacional, la defensa y los conflictos armados tanto totales como limitados.

En un esfuerzo por ayudar a aclarar y mejorar el entendimiento del papel que juega o puede llegar a jugar el ciberespacio en los ámbitos de la seguridad nacional, la defensa y la guerra, este análisis se concentrará en evaluar las posibilidades y el alcance que pueda o no llegar a tener el ciberespacio en el concepto tradicional de la guerra moderna y futura, ya sea ésta convencional o asimétrica, total o limitada.

Cuando hablamos de una guerra en abstracto, el concepto tradicional que se tiene es el de un conflicto estilo Segunda Guerra Mundial, con despliegues de cientos de miles de hombres, tanques, aviones y cañonazos a gran escala de ambos bandos. A este tipo de conflicto se le conoce como guerra convencional, pues se da entre naciones con capacidades militares similares; sin embargo, el tipo de conflictos armados que han ocurrido desde el final de la Segunda Guerra Mundial han sido en su mayoría de tipo no convencional o asimétrico, es decir, entre una nación y un grupo criminal, terrorista, o insurgente, o entre una nación con capacidades militares significativamente superiores a las de su rival.

Guerras como Vietnam, Corea, Argelia, Irak, Afganistán y Siria son ejemplos representativos del tipo de conflictos más comunes de las últimas décadas. La característica más distintiva de estas guerras – en comparación con, por ejemplo, las dos guerras mundiales – es el uso limitado de los elementos de poder, especialmente los militares, por parte de al menos uno de los bandos. Existen varias razones para la limitación de dichos elementos de poder. Por un lado, los principios de la guerra justa dictan que el nivel de fuerza utilizado debe ser proporcional a los objetivos que se buscan alcanzar. Es decir, si se busca, por ejemplo, derrotar a un grupo terrorista como el Estado Islámico, sería desproporcionado lanzar bombas nucleares sobre todo el Oriente Medio.

Por el otro lado, la cuerda sobre la que se balancean las relaciones políticas y diplomáticas de los países entre quienes existen tensiones, es muy delgada. Las tensiones que existen entre potencias militares como EEUU, China, Rusia, Turquía, Japón y Corea del Norte deben ser navegadas con extremo cuidado, pues la

tecnología armamentística y militar de hoy en día, ha alcanzado una capacidad de destrucción sin precedentes y difícil de imaginar. El problema radica en que, a pesar del riesgo de desatar un conflicto armado convencional de alta intensidad (pensemos en una Tercera Guerra Mundial), las grandes potencias mundiales aún tienen intereses y agendas políticas que perseguir, y el poderío militar es, aunque no siempre la primera herramienta de coerción o disuasión a la que recurren las naciones, sí es la más relevante y poderosa, y por tanto se suele dejar como último recurso una vez que todas las demás herramientas de negociación hallan fallado.

Es importante entender el concepto de la disuasión, pues incluso cuando un grupo o nación ha llegado al punto de amenazar con tomar acción militar contra algún rival, la verdadera intención de la amenaza es la de coercer o disuadir a dicho rival a través de la intimidación, para así conseguir imponer la voluntad del grupo o país agresor sobre la del rival sin necesidad de un conflicto armado. El riesgo que se corre es que, durante la amenaza de acción militar – que por lo general involucra el despliegue de tropas, militarización de fronteras, movilización de reservas, ejercicios militares, ruptura de relaciones diplomáticas, etc. – se cometa algún acto hostil que el rival considere como inaceptable y esto provoque que la amenaza escale a un conflicto armado abierto.

Este tipo de escenarios ilustran algunas de las dinámicas actuales de la guerra moderna, sin embargo, y como este análisis pretende demostrar, el creciente dominio del ciberespacio ofrece alternativas y posibilidades no antes disponibles y que, dependiendo de los actores involucrados y el contexto de cada conflicto, pueden abrir opciones que cambien la manera en que pensamos, conceptualizamos y actuamos en los conflictos armados modernos y futuros.

Para lograr el objetivo de este análisis, primeramente, se analizarán dos condiciones esenciales para que un dominio emergente, como el ciberespacio, pueda realmente tener un impacto relevante en la guerra y por tanto en el concepto bajo el que pensamos sobre la misma. Una vez establecida la viabilidad del ciberespacio para cumplir con ambas condiciones, se analizará un estudio de caso que apoye los argumentos y condiciones previas. Posteriormente, y basado en precedentes reales, se explorará el impacto específico que el ciberespacio podría tener en los elementos críticos de un grupo o nación entablado en un conflicto armado o en el preámbulo de uno. Finalmente, se aclararán algunas características del ciberespacio y de los escenarios analizados para poner el fenómeno completo en una perspectiva objetiva.

DOS CONDICIONES PARA IMPACTAR LA PRÁCTICA DE LA GUERRA

La práctica de la guerra, así como las estrategias y tácticas que la guían, han cambiado y evolucionado constantemente de la mano de la época en que se desenvuelven. En la mayoría de los casos, ha sido un arma o tecnología de combate la que ha propiciado la evolución del conflicto armado.

Ejemplos hay por doquier. La invención del carro de guerra permitió a civilizaciones como la Egipcia, Asiria o Hitita una movilidad en el campo de batalla sin precedentes, que obligó a sus rivales a evolucionar y adaptarse a la nueva forma de guerrear. La pólvora revolucionó la práctica de la guerra, desde la capacidad de desplegar gran cantidad de soldados que con poco entrenamiento eran capaces de asestar disparos letales a oponentes a través de la concentración del fuego, hasta la capacidad de derribar murallas y fortificaciones utilizando artillería de pólvora.

Las aeronaves cambiaron la práctica de la guerra desde el nivel táctico hasta el estratégico; la superioridad aérea se volvió la prioridad de cualquier operación militar que pretendiera dominar territorio en tierra, aire o mar. Las armas nucleares cambiaron la práctica y conceptualización de la guerra a tal grado que en los años 80s, tras décadas de la carrera de las armas entre los Estados Unidos y la Unión Soviética, analistas militares comenzaron a hablar del "fin de la estrategia", como resultado de aparentemente haber llegado a un punto donde el conflicto armado ya no era posible sin provocar como consecuencia una destrucción mutua asegurada y probablemente un holocausto nuclear que pusiera en riesgo la supervivencia de la humanidad.

Estos son sólo algunos ejemplos que hacen evidente un patrón: la tecnología y evolución de las armas tienen la capacidad de impactar y cambiar la práctica y concepto de la guerra.

Bajo dicha premisa, los dos puntos a considerar en este análisis son, primero, si la tecnología que ha permitido el auge del ciberespacio puede ser considerada y utilizada como un arma; y segundo, si el ciberespacio puede tener efectos físicos, o en el "mundo real", que lo conviertan en un arma capaz de impactar el concepto de la guerra.

EL CIBERESPACIO COMO ARMA

Un arma es, sencillamente, un instrumento utilizado para causar daño. Desde lanzas para cazar, instrumentos para torturar o bombas para destruir, el ser humano ha desarrollado estas armas para distintos contextos, pero siempre con el fin de provocar algún tipo de daño a un objetivo en particular.

Por ende, podemos definir un arma como una herramienta que es utilizada, o diseñada con el objetivo de causar daño físico, funcional o mental a estructuras, sistemas o seres vivientes (Rid & McBurney, 2012, p. 7).

En el contexto del ciberespacio, el "mundo virtual" está construido a partir de código de computadora, convirtiéndolo a éste en su herramienta principal. Considerando que el código de computadora es la herramienta del ciberespacio, la siguiente pregunta a considerar es ¿si dicha herramienta puede ser utilizada como un arma?

Para contestar esta pregunta, es necesario considerar el aspecto psicológico de las armas. La mayoría de las herramientas utilizadas por el ser humano no han sido diseñadas con el propósito de causar daño. Sin embargo, muchas de dichas herramientas pueden ser utilizadas para hacerlo, convirtiéndose así en armas. Es entonces que la intención de dañar o de amenazar con causar daño es lo que realmente cataloga a un objeto como arma.

Así como el hacha de un leñador o los puños de un artista marcial no son armas en sí mismas, el código de computadora tampoco lo es. Es en el momento que hay una intención de causar daño que estas herramientas se convierten en armas. Bajo este entendimiento, se puede definir un arma cibernética como un código de computadora que es utilizado o diseñado con el objetivo de causar daño físico, funcional o mental a estructuras, sistemas o seres vivientes (Rid & McBurney, 2012, p. 7).

Así como un arma – en este caso, un arma cibernética – se considera como tal por la intención de infligir daño a un objetivo, es importante también considerar las dinámicas que se generan a partir de la sola amenaza de causar dicho daño.

Bajo un escenario de amenaza, un "arma" puede causar los efectos deseados sobre su objetivo sin necesidad de causar daño. Lo que esta dinámica refleja es que independientemente de la intención del agresor, la percepción que la víctima tenga sobre la amenaza y la capacidad de dicha amenaza de provocarle daño, puede convertirla automáticamente en un arma, incluso si el atacante no la ve como tal.

A esta dinámica se le conoce como el efecto de la pistola de paintball (Rid & McBurney, 2012, p. 8). Si, por ejemplo, un asaltante porta una pistola falsa para intentar robar un banco, a la hora de cometer el asalto, basta con que las víctimas crean que la pistola que porta es real para que surja el efecto que el asaltante desea, pues incluso cuando él sabe que su herramienta no es un arma real, sí se le puede considerar como tal ya que está logrando el mismo objetivo que lograría un arma real. Por el contrario, si las víctimas se percatan de que la pistola es falsa, la herramienta deja de ser un arma y pierde su efecto coercitivo sin importar la intención del asaltante de pretender utilizarla como un arma.

Es importante comprender estas dos dinámicas psicológicas, pues es a través de ellas que una herramienta como el código de computadora, que en esencia no es un arma, puede convertirse en una, ya sea por la intención del agresor o por la percepción de la víctima. Bajo estas condiciones es que podemos afirmar que el código de computadora – y, por ende, el ciberespacio – sí puede ser percibido y utilizado como un arma.

LOS EFECTOS FÍSICOS DEL CIBERESPACIO

Un argumento que gran número de ciber-escépticos constantemente utilizan para apoyar su ideología es el que sugiere que al ser el ciberespacio un ente digital, éste es incapaz de tener efectos directos en el mundo

físico, por lo que su utilidad y alcance se limitan al mundo cibernético y como mera herramienta de apoyo a aquellos entes que sí existen y operan en el espacio físico o "mundo real".

En su prominente artículo *Cyber War Will Not Take Place* ("La Ciberguerra No Tendrá Lugar"), el académico y experto en el ciberespacio Thomas Rid argumenta que la guerra cibernética nunca ha ocurrido ni ocurrirá bajo la premisa de que el código de computadora, la herramienta principal del ciberespacio, es un ente digital que por su misma esencia no puede tener repercusión alguna en el mundo físico. Rid argumenta que el alcance de un ataque cibernético se limita a actividades comunes como el sabotaje, el espionaje y la subversión. Rid también argumenta que los ataques cibernéticos no cumplen con las características necesarias para considerarlos actos de guerra; siendo estas principales características la ausencia del principio de letalidad y la capacidad de aplicar coerción para conseguir objetivos políticos a través del uso de código de computadora.

Conceptualizaciones como la de Rid sirven para ilustrar el consenso general que se suele tener acerca de la naturaleza de los ataques cibernéticos. Es entendible que el tipo de actividades que Rid sugiere – sabotaje, espionaje y subversión – reciban tanta atención como lo hacen, pues son el tipo de operaciones cibernéticas más comunes. Las estadísticas son claras:

- En 2017, se registró, en promedio, un ciber ataque cada 39 segundos (Cybint, 2017).
- Desde 2013, 3,809,448 archivos han sido robados tan solo en los EEUU como resultado de infiltración por hackers a sistemas de información (Cybint, 2017).
- Según el FBI, los ataques de tipo *ransomware* – que involucran el bloqueo de acceso a computadoras o información hasta que se pague un rescate – son el tipo de ataques más prominentes hoy en día, llegando a una cifra de más de 4,000 ataques diarios tan solo en los EEUU (Federal Bureau of Investigation, 2017).

Es claro que, en su gran mayoría, los ataques cibernéticos tienen como objetivo la extracción o manipulación de la información. Si se considera que dicha información se encuentra en el "mundo virtual", es entonces entendible que el argumento de Rid acerca de la incapacidad del código de computadora de tener efectos en el mundo físico sea comúnmente aceptado como válido.

Si se acepta el argumento de Rid, es entonces difícil pensar que el ciberespacio pueda tener un alcance o aplicación tal que impacte el concepto tradicional de la guerra, que primordialmente se desenvuelve en el espacio físico o "mundo real". Bajo su premisa, el ciberespacio se convierte simplemente en una herramienta y un multiplicador de fuerza.

Una de las consecuencias que generan estadísticas como las anteriores, es la de crear una visión de túnel sobre las amenazas cibernéticas y concentrarse exclusivamente en el mundo digital y la información que

reside en él. El riesgo de este patrón, es que otras estadísticas que, aunque más pequeñas, no son menos relevantes, pasan prácticamente desapercibidas.

Una de dichas estadísticas es la de un fenómeno conocido como la ciber-cinética, es decir, los efectos físicos – en el "mundo real" – que puede tener una operación o ataque cibernético y que usualmente se considera mera ciencia ficción, o, como asumirían los ciber-escépticos, sin relevancia o impacto alguno en la vida cotidiana.

La ciber-cinética se define como una clase de ataque cibernético que puede causar daño físico directa o indirectamente, lesiones, e incluso la muerte exclusivamente a través de la explotación de sistemas de información y procesos vulnerables (Applegate, 2013, p. 1).

Las estadísticas de la ciber-cinética, aunque pequeñas, son substanciales. Marin Ivezic, presidente del Instituto de Ciber-Cinética de Hong Kong se ha dado a la tarea de recopilar una lista con la mayor cantidad de incidentes ciber-cinéticos, desde el primero del que se tiene información, ocurrido en 1982. Dichos incidentes abarcan desde accidentes, mal funcionamientos y experimentos en laboratorios controlados, hasta disrupciones deliberadas, ciber-crímenes y ataques de Amenaza Persistente Avanzada. Al día de hoy, Ivezic ha logrado recopilar apenas poco más de 50 incidentes en total; por un lado, debido a que la frecuencia de incidentes ciber-cinéticos es baja, y por el otro, debido a que un gran número de estos incidentes no se reportan a las agencias encargadas de investigarlos.

Estadísticamente, éste es un número insignificante en comparación con el enorme número de incidentes de espionaje y subversión que ocurren por millares día tras día. Sin embargo, tras el episodio de Stuxnet ocurrido en Irán en 2009 y que exploraremos más adelante en este análisis, ignorar, desconocer o no tomar seriamente las amenazas ciber-cinéticas, podría convertirse próximamente en el riesgo de seguridad más grande para las agencias de ciberseguridad, gobiernos, empresas privadas y fuerzas armadas, además de que es un fenómeno con potencial de cambiar algunas dinámicas del concepto tradicional de la guerra antes descrito.

¿Cómo es posible la ciber-cinética? A través de los Sistemas Físico-Cibernéticos (SFC). Un SFC se refiere a la conjunción y coordinación entre recursos computacionales y físicos, es decir, la integración de sistemas computacionales en procesos físicos (Applegate, 2013, p. 1). Ejemplos de SFC nos rodean en la vida cotidiana: aparatos médicos, controles de tráfico y vialidad, aviación, energía eléctrica, controles de abastecimiento de agua, comunicaciones, manufacturas, fábricas y maquiladoras, y hasta sistemas de defensa. Lo que éstos y otros ejemplos tienen en común, es que todos son sistemas que monitorean o manejan procesos físicos en el "mundo real", a través de sistemas computacionales que controlan dichos procesos.

La prominencia y utilización de SFC se incrementa día con día en gran parte por la motivación de que los procesos físicos y sistemas conectados cibernéticamente operan más eficientemente, recolectan más información y expanden su capacidad funcional de esa manera (Ivezic, 2017b). En términos prácticos, conectar cada pieza de equipo al ciberespacio permite que la información disponible en una red abierta pueda ser accesible a aquellos encargados de controlarlas en cualquier momento y sin importar el lugar en que se encuentren. Mientras más sistemas estén interconectados entre sí, más eficiente es su operación y accesibilidad; sin embargo, dichos beneficios vienen acompañados de un creciente riesgo.

El problema es simple de entender. Un SFC está diseñado para tener efectos cinéticos, en el "mundo real", y el funcionamiento de un SFC es controlado por un sistema de computadoras que, como vimos anteriormente, funciona a partir de código de computadora. Por lo tanto, al contener código de computadora, el sistema computacional está operando en el ciberespacio, y dada la interconectividad de dichos sistemas computacionales con los SFC que éstos controlan, es posible manipular cibernéticamente dichos sistemas computacionales para utilizar los SFC con propósitos distintos para los que fueron diseñados.

Desafortunadamente, la eficiencia y accesibilidad que permiten los SFC ha llevado a que la mayoría de las industrias que los utilizan se concentren en conectar más y más sistemas entre sí, incrementando la eficiencia y accesibilidad de sus operaciones, e ignoren la seguridad de dichos sistemas. Una suposición que se encuentra fuertemente arraigada entre aquellos que diseñan y utilizan SFC es la que se conoce como "seguridad por obscuridad", que se refiere a la idea de que los sistemas operativos que utilizan los SFC son tan distintos y ajenos a los que la mayoría de otros sistemas utilizan, que los hackers no gastarían su tiempo tratando de aprenderlos y buscando maneras de explotar sus vulnerabilidades. La realidad es que la unicidad de los SFC no ha sido un impedimento para aquellos que pretenden infiltrar y manipular dichos sistemas.

Una vez comprendida la interconectividad que existe entre sistemas físicos y sistemas computacionales en forma de SFC y los riesgos que ésta conlleva, podemos afirmar que el ciberespacio, a través de un fenómeno como la ciber-cinética, tiene en efecto la capacidad de generar efectos físicos, en el "mundo real". Para reforzar este argumento, analizaremos el ejemplo más relevante con que se cuenta hasta el día de hoy.

ESTUDIO DE CASO

Ataques ciber-cinéticos han ocurrido ya en distintas ocasiones y han provocado daño físico a plantas nucleares, plantas de agua, pipas de petróleo, fábricas, hospitales, sistemas de transporte, edificios habitacionales, entre otros. Como se mencionó anteriormente, la principal razón por la que este tipo de ataques no reciben tanta atención y cobertura por parte de los medios o la comunidad de ciber-seguridad es por la naturaleza dispersa y poco común de estos incidentes.

Sin embargo, basta analizar algunos de los ataques e incidentes ciber-cinéticos que se han suscitado en las últimas décadas para comprender la seriedad y el enorme alcance que este tipo de ataques podría llegar a tener tanto en la vida cotidiana como en un conflicto armado.

STUXNET

En 2010, el mundo conoció a la que ha sido considerada la primera verdadera arma cibernética: el gusano Stuxnet. Con una estructura extraordinariamente compleja de más de 150,000 líneas de código, Stuxnet es hasta hoy uno de los códigos maliciosos más sofisticados jamás creados.

Stuxnet fue descubierto a mediados del año 2010 por una pequeña empresa de seguridad en Belarús llamada *VirusBlokAda*. A pesar de que miles de virus y programas maliciosos son descubiertos y reportados diariamente por todo el mundo, Stuxnet recibió especial atención cuando Microsoft confirmó que el gusano estaba infiltrando computadoras utilizadas para manejar sistemas de controles industriales a gran escala que utilizaran el sistema operativo Windows.

Dichos sistemas se conocen como Controles de Supervisión y Adquisición de Datos (SCADA por sus siglas en inglés) y son utilizados para controlar las operaciones de industrias como plantas de energía y fábricas hasta pipas de petróleo e instalaciones militares. Con esto en mente, y para comprender el extraordinario diseño de Stuxnet, es necesario mencionar lo específico que fue la creación de esta arma cibernética.

La gran mayoría de los virus de computadora tienen como objetivo final el infectar al mayor número de computadoras posibles y ejecutar la misión para la que fueron programados en tantos sistemas como les sea posible. Por lo general estas misiones involucran el robo o manipulación de información, contraseñas, disrupciones, y recientemente, “secuestro” de información valiosa por la que los criminales exigen el pago de un rescate para devolver el acceso a dicha información a sus dueños. En términos generales, se trata de propagar el virus indiscriminadamente y causar daño a todas aquellas computadoras que se logren infiltrar.

Stuxnet fue diferente. El gusano Stuxnet, a pesar de que infectó a más de 200,000 computadoras, fue diseñado para no causar ningún tipo de daño en ellas a menos que ciertos requisitos fueran cumplidos. Lo que esto indica es que Stuxnet no era un gusano cualquiera que buscaba infectar indiscriminadamente y dañar a tantas computadoras como pudiera; Stuxnet estaba en búsqueda de un objetivo muy específico. Este tipo de ataques se conocen como Ataques de Amenaza Persistente Avanzada y se caracterizan por ser difíciles de prevenir o detener, ya que una vez que el código malicioso haya logrado penetrar una red, éste está diseñado para no ser detectado por la mayor cantidad de tiempo posible, el cual aprovecha para llevar a cabo su misión (Musa, 2014).

Una vez que Stuxnet y sus intrincaciones fueron descubiertas, investigadores de las empresas de seguridad cibernética Kaspersky y Symantec comenzaron a trabajar para profundizar en el diseño del código y

comprender su funcionamiento. Es gracias al trabajo de dichos investigadores que hoy conocemos con alta precisión el modelo de operación de la primera arma cibernética.

El proceso comenzaba cuando dispositivos USB que estaban infectados con el gusano Stuxnet eran conectados a computadoras dentro de plantas o industrias. Curiosamente, el método utilizado para lograr esto fue colocar dichos dispositivos USB en los estacionamientos de empleados de las plantas o industrias, quienes, al encontrarlos y recogerlos, tendrían la curiosidad de conocer los contenidos del dispositivo.

Una vez que el USB infectado se conectaba a una computadora, Stuxnet infiltraba la red interna de la planta o industria y comenzaba a propagarse de una computadora a otra hasta encontrar aquellas computadoras que manejaran los sistemas de control industrial. Una vez que Stuxnet encontrara una de dichas computadoras, el gusano comenzaba a buscar si el programa *Step 7*, diseñado por la compañía Siemens, estaba instalado en esa computadora. De ser así, Stuxnet hackeaba el programa utilizando una contraseña secreta codificada ya dentro de *Step 7*.

Una vez hackeado, Stuxnet buscaba si, a través de *Step 7*, esa computadora tenía un sistema de control conocido como Controlador Lógico Programable (PLC por sus siglas en inglés). Este controlador es un sistema que se utiliza para comunicar a la computadora con una máquina física. El PLC traduce los comandos que da la computadora para que la máquina física los ejecute. Si Stuxnet encontraba dicho PLC en una computadora, tomaba control de él también.

Una vez que Stuxnet controlaba el PLC, el código buscaba qué componentes eléctricos estaban conectados al mismo. Específicamente, Stuxnet buscaba la presencia de dos microchips fabricados por las compañías *Vacon*, de origen Finlandés, y *Fararo Paya*, de origen Iraní, cuyo trabajo era el de controlar la velocidad de rotación de los motores de una máquina. Si Stuxnet no encontraba estos microchips, o si los chips encontrados pertenecían a otra compañía, el gusano detenía sus operaciones y se auto-eliminaba de la computadora.

En caso de que Stuxnet sí encontrara ambos microchips, comenzaba entonces a buscar la velocidad específica a la que giraban los motores conectados a ambos microchips. Específicamente, Stuxnet buscaba aquellos motores girando a velocidades de entre 807 Hz y 1,210 Hz. De nuevo, si Stuxnet no encontraba dichos motores, o si la velocidad estaba fuera del rango que buscaba, el gusano terminaba sus operaciones y se auto-eliminaba de la computadora.

Los investigadores que lograron descifrar este proceso a través del análisis del código de Stuxnet comenzaron entonces a preguntarse qué plantas, fábricas o industrias podrían tener máquinas con las características exactas que Stuxnet buscaba. Tras su análisis y búsqueda, los investigadores encontraron un

lugar que poseía todas las características que buscaba Stuxnet: un centrifugador de gas en una planta de enriquecimiento de uranio ubicada en Natanz, Irán.

Fue entonces que los investigadores comenzaron a conectar los puntos. El uranio enriquecido es el material principal utilizado en la fisión nuclear, que es el proceso que se lleva a cabo en plantas nucleares, pero también en bombas nucleares. Para lograr dicho proceso de enriquecimiento, el método más común es utilizar un centrifugador de gas, el cual se compone de tubos que rotan a grandes velocidades y a los cuales se les inyecta gas de uranio a altas temperaturas para que las fuerzas centrífugas separen los isótopos del uranio y el producto final que se obtenga de los tubos sea uranio enriquecido.

El objetivo de Stuxnet fueron precisamente los PLC que controlaban los motores que hacían rotar los centrifugadores de gas. Si Stuxnet encontraba en una computadora todos los requisitos antes mencionados, el código del gusano modificaba la velocidad a la que giraban los centrifugadores. En un inicio aceleraba la rotación para después bajarla considerablemente y finalmente devolverla a su velocidad normal. Stuxnet ejecutaba estos cambios de velocidad en los centrifugadores una vez cada 27 días. Considerando que los centrifugadores de gas rotan normalmente a velocidades de decenas de miles de revoluciones por minuto a altas temperaturas, cualquier modificación que altere su sensible funcionamiento normal puede ser desastrosa.

Es entonces que los efectos ciber-cinéticos de Stuxnet se vuelven evidentes. En el mejor de los escenarios, los centrifugadores de gas se desgastarían más rápido de lo normal y tendrían que ser reemplazados, lo cual conllevaría un costo significativo; en el peor de los escenarios, los centrifugadores se desintegrarían en pedazos. Al alterar las velocidades de rotación de los centrifugadores y provocar turbulencias en los mismos, Stuxnet logró el peor de los escenarios y se estima que aproximadamente 1,000 centrifugadores fueron destruidos y sus reemplazos solicitados por el gobierno Iraní (Albright, 2010, p. 1).

Es importante recalcar las propiedades de Stuxnet como Amenaza Persistente Avanzada, pues a pesar de estar manipulando las velocidades de rotación de los centrifugadores, los ingenieros de la planta no lograban descifrar lo que estaba sucediendo. El código de Stuxnet había sido programado para que, al alterar las velocidades de los rotadores, la información que se mostrara en los monitores de las computadoras que controlaban dichos rotadores fuera la normal; Stuxnet estaba disfrazando sus propias manipulaciones hasta que era ya demasiado tarde para hacer algo al respecto. Hasta donde los ingenieros podían ver, los motores estaban rotando a velocidades normales y seguras, pero en realidad, Stuxnet estaba manipulando esas lecturas para mantener sus operaciones ocultas.

EL ALCANCE DE LA CIBER-CINÉTICA EN LA GUERRA

Stuxnet es sin duda el ejemplo más contundente hasta la fecha de lo que la ciber-cinética es capaz de hacer. Como ha sucedido a lo largo de la historia, una vez más estamos frente a una tecnología que, combinada con el contexto y prácticas de las fuerzas armadas actuales y futuras, tiene el potencial de generar dinamismos capaces de impactar el concepto y dinámica de los conflictos armados modernos.

La mayor parte de la evidencia apunta a que la creación y el ataque de Stuxnet fue una operación conjunta entre los EEUU e Israel contra Irán. Los resultados del ataque fueron claros: el programa de armamento nuclear Iraní se retrasó por varios años y la moral de sus ingenieros fue severamente afectada al hacerles creer que eran incapaces de manejar la planta de enriquecimiento (Nakashima, 2012).

Inicialmente puede resultar difícil imaginar cómo es que un ataque como Stuxnet, que a pesar de su extraordinario diseño y ejecución sin precedentes, puede impactar las dinámicas de un fenómeno tan complejo y vasto como la guerra. Por un lado, se puede argumentar que el alcance de Stuxnet fue limitado, ya que sólo afectó una pequeña parte de las capacidades militares Iraníes – su programa nuclear – mientras que el resto de sus fuerzas armadas permanecieron intactas al ataque de Stuxnet. Por otro lado, también se puede argumentar que el ataque de Stuxnet no involucró letalidad, que en la estrategia militar es usualmente el primer indicador a considerar cuando se evalúan los costos y riesgos aceptables e inaceptables que un grupo o nación están dispuestos a absorber en la persecución de sus objetivos.

Para hacer una antítesis de dichos argumentos, es necesario remitirse a los principios. Si el argumento de este análisis dicta que el ciberespacio tiene el potencial de impactar dinámicas fundamentales de la guerra moderna y futura, consideremos entonces los principios fundamentales de la misma.

La guerra, como instrumento político, tiene en su forma más abstracta un solo objetivo: coercer o disuadir al enemigo para imponer una voluntad política sobre él. Toda estrategia, operación, táctica o principio de la guerra es una herramienta que tiene como propósito acercar al actor que la utiliza a alcanzar el punto en el que pueda coercer o disuadir a su enemigo de continuar peleando, o de siquiera iniciar dicha pelea, e imponer su voluntad, usualmente política, sobre él (Stone, 2015).

Considerando la premisa anterior, es entonces necesario analizar la capacidad que pueda o no tener el ciberespacio para coercer o disuadir a un enemigo y poder así imponer su voluntad sobre él. Para hacer dicho análisis, enlistemos los principales elementos que un grupo o nación usualmente requiere quebrantar al nivel estratégico para coercer o disuadir a un enemigo:

1. Población: es el fundamento de cualquier grupo o nación entablado en un conflicto armado, sobre todo en un escenario de guerra total, más que en uno de guerra limitada. Conforma el núcleo de las fuerzas armadas, la economía, la producción, la logística y, sobre todo, es el elemento vital para perpetuar la

supervivencia del grupo o nación, incluso ante una derrota militar. Cabe mencionar que el quebrante de una población se puede dar no sólo como resultado de la aniquilación parcial o total de sus miembros, sino también por la simple falta de voluntad de los mismos a continuar peleando; básicamente, quebrantar la moral que conlleve a una rendición.

2. Fuerzas Armadas: es la principal línea de defensa de cualquier grupo o nación entablado en conflicto armado. En esta categoría se consideran no solo los efectivos humanos, sino también los efectivos no-humanos como drones, robots o sistemas de defensa autónomos capaces de combatir. Cabe mencionar que hoy en día, la doctrina militar por la que potencias militares como EEUU, Rusia o India están apostando, es la doctrina de Operaciones Centradas en la Red (*Network-centric Warfare*), explicada más adelante.

3. Economía: es el oxígeno de cualquier esfuerzo de la guerra. Sin los recursos necesarios para sostener la producción y funcionamiento de armas, vehículos, dispositivos y herramientas; la alimentación, sustento y abastecimiento de tropas y civiles; el comercio de recursos y materiales escasos o no disponibles para el grupo o nación; así como la estabilidad económica interna suficiente para perpetuar la supervivencia y continuación del grupo o nación, incluso ante una derrota militar, se vuelve una decisión extremadamente arriesgada continuar involucrado en un conflicto armado. Cabe mencionar que hoy en día, el frente económico es uno de los principales recursos que las potencias mundiales utilizan para coercer y disuadir a sus rivales sin necesidad de escalar a un conflicto armado. Claros ejemplos son los embargos y sanciones económicas que se han impuesto a países como Cuba, Rusia y Corea del Norte.

4. Producción y logística: en la estrategia militar existe un famoso refrán que dice: “Los principiantes hablan de estrategia; los profesionales hablan de logística”. Lo que el refrán refleja es la crucial importancia que tiene la producción y la logística en cualquier esfuerzo armado. Por un lado, sin una producción capaz de satisfacer la necesidad y demanda de armas, vehículos, dispositivos, municiones, herramientas, provisiones y personal que requiere un conflicto armado, es mera cuestión de tiempo para que ese grupo o nación sea incapaz de seguir combatiendo. Por el otro lado, una capacidad de producción suficiente es poco útil si no se cuenta con una sólida cadena de logística que permita que todo lo que se produce llegue al lugar en que se necesita y esté disponible en el momento que se necesita.

5. Unidad nacional: es peculiar sugerir que, para los EEUU, la guerra de Vietnam se perdió no en las junglas del sudeste asiático, sino en los hogares de Norteamérica. Un conflicto armado requiere no sólo un esfuerzo militar, sino también un esfuerzo civil que, dependiendo de la escala del conflicto, puede cambiar totalmente la vida cotidiana de la sociedad en casa. En la estrategia militar se pone un gran énfasis en la idea de que una guerra se pelea tanto en el frente de combate como en el frente doméstico.

Sin el apoyo, cooperación, disposición y fuerza de voluntad de la sociedad civil, es difícil que una nación democrática, como son la mayoría de las naciones Occidentales, pueda iniciar o continuar un conflicto armado sin violar sus principios democráticos.

6. Élites políticas o militares: el proceso democrático que países como EEUU o México siguen hoy en día para hacer una declaración de guerra – a través del Congreso o la Cámara de Diputados, respectivamente – es un proceso que cae más en el lado de la excepción que de la regla. Históricamente, las facultades y la decisión de participar o no en un conflicto armado han sido, en su mayoría, unilaterales y concentradas en élites políticas y militares como reyes, emperadores, jefes o generales y su cercano círculo de allegados. En tiempos modernos aún hay ejemplos de este fenómeno unilateral, desde la Alemania Nazi de Adolfo Hitler hasta la República de Corea del Norte de Kim Jong-un. Sin embargo, este fenómeno es un arma de doble filo. Si bien dichas élites políticas o militares concentran la mayoría del poder en ellas, esto también las convierte en una pieza *sine qua non,* es decir, sin la cual su ideología y pretensiones políticas o militares difícilmente pueden continuar.

Estos seis elementos descritos son algunos de los principales centros de gravedad que un grupo o nación suele tener. Un centro de gravedad, como lo describe su autor original - el militar y teórico de la guerra prusiano, Carl von Clausewitz – es el centro de todo el poder y movimiento sobre el cual depende todo (Clausewitz, 1993, p. 720). Es importante aclarar la errónea noción común de que un centro de gravedad es la fuente de fuerza o poder de alguna entidad; aunque en ocasiones sí pueden converger en el mismo objeto, el centro de gravedad es en realidad un elemento de balance más que de fuerza. Por lo tanto, si se ataca un centro de gravedad con suficiente fuerza, éste perderá su balance y, al ser el elemento en el cual converge la estabilidad de toda la estructura, ésta colapsará de igual manera.

El centro de gravedad de un grupo o nación en conflicto armado es subjetivo a los actores y al contexto de cada situación; incluso, el centro de gravedad puede cambiar constantemente a lo largo de un mismo conflicto armado. Sin embargo, lo relevante para este análisis es identificar los seis centros de gravedad antes descritos y cuya pérdida de su balance resultaría, con altas probabilidades, en la incapacidad o falta de voluntad del grupo o nación para seguir combatiendo o siquiera iniciar el conflicto armado, es decir, coerción o disuasión respectivamente.

ESCENARIOS

Con la comprensión de los conceptos y antecedentes ya presentados es que finalmente podemos cerrar el círculo de este análisis y explorar el impacto que el ciberespacio, a través de fenómenos como la ciber-cinética y algunos de sus precedentes más relevantes, puede tener en las dinámicas y conceptualización de

la guerra moderna con base en la capacidad y potencial de desbalancear los centros de gravedad ya identificados.

POBLACIÓN Y UNIDAD NACIONAL

Comencemos con los centros de gravedad de población y unidad nacional, estrechamente vinculados uno a otro y que en su mayoría se refieren a la sociedad civil que actúa en el frente doméstico. Como se mencionó anteriormente, el quebrante o desbalance de estos centros de gravedad se ha dado históricamente más por la desmoralización y renuencia de la población a continuar o iniciar un conflicto armado que por el exterminio total o parcial de la misma. Con dicho patrón en mente es que la ciber-cinética puede jugar un rol significativo en el proceso de desmoralización de un grupo o población y con ellos, la unidad y apoyo nacional.

El proceso de desmoralización de un grupo o nación ocurre paulatinamente. Es más un proceso paulatino y constante de pequeños incidentes más que un gran incidente único, como por ejemplo, la detonación de armas nucleares sobre Japón durante la Segunda Guerra Mundial y que fue, aunque no el único, el factor decisivo para su rendición tan solo unos días después.

Dicho esto, el proceso de desmoralización usualmente ocurre a través de un desgaste físico, pero sobre todo mental y emocional del grupo o población. Una de las tácticas utilizadas en la guerra psicológica para dicho fin es la de mantener a la víctima en constante estado de alerta y peligro. El efecto de esta táctica es el desgaste físico y emocional de las víctimas. Por ejemplo, durante la Segunda Guerra Mundial, las alarmas que sonaban para advertir a la población de un bombardeo inminente creaban pánico y caos entre la población. Los efectos fueron severos, pues se conocen miles de casos de individuos con Trastorno de Estrés Postraumático (TEPT) que incluso después de la guerra sufrían crisis nerviosas y ataques de pánico al escuchar cualquier alarma o sirena.

La ciber-cinética tiene la facultad de crear situaciones similares. En 2017, un hackeo al sistema de alarmas de tornados en Dallas, Texas, provocó que 156 sirenas de emergencia sonaran durante varios minutos, despertando y alterando a la población de la ciudad (Newman, 2017). Como incidente aislado y que ocurra una sola vez, el efecto puede ser prácticamente irrelevante. Sin embargo, como se mencionó anteriormente, la constante y paulatina práctica de este tipo de ataques es lo que puede provocar un desgaste físico y mental en las víctimas, y con ello, su desmoralización.

En la misma Ciudad de México se pueden observar los efectos que un ataque de esta naturaleza podría tener. Tras los fuertes sismos de septiembre de 2017 y febrero de 2018, es innegable que se ha generado una paranoia y estrés colectivo entre los habitantes de la ciudad, mismos que se desencadenan cada vez que suena la alarma sísmica. En un escenario en el que un grupo o nación hostil a México quisiera explotar dicha situación, hackear y hacer sonar las alarmas sísmicas constantemente o durante la noche,

interrumpiendo así el sueño y descanso de los habitantes de la ciudad, puede desgastar muy rápidamente la estabilidad física y emocional de la ciudad más importante del país.

Similarmente, los ataques ciber-cinéticos tienen el potencial de afectar severamente la calidad de vida de las víctimas, lo cual suma indiscutiblemente al efecto desmoralizante. A finales de 2015, un grupo de hackers rusos conocidos como *Sandworm*, lanzó un ataque ciber-cinético contra la planta eléctrica de Prykarpattyaoblenergo, en el oeste de Ucrania (Stone, 2016). Las motivaciones son claras. Tras la anexión de Crimea, una región del sur de Ucrania, a Rusia en 2014, los principales opositores de la anexión fueron las ciudades del oeste de Ucrania, que por su cercanía geográfica con Europa Oriental se identificaban más como pro-europeos que como pro-rusos. Rusia, en respuesta a la oposición de dicha región del oeste de Ucrania, patrocinó este ataque ciber-cinético que dejó sin electricidad a más de 80,000 personas durante al menos seis horas.

De igual manera, como incidente aislado puede no tener gran repercusión; sin embargo, ataques similares constantes contra plantas eléctricas pueden causar severos estragos entre una población: las comunicaciones se ven directamente afectadas; numerosos servicios públicos se detienen; medios de vialidad y transporte dejan de funcionar; en los hogares, alimentos perecederos comienzan a echarse a perder a falta de la refrigeración adecuada; aumenta el crimen y el orden público se debilita ante la disminuida capacidad de respuesta de las autoridades. Estos son algunos escenarios posibles que un ataque ciber-cinético de esta naturaleza podría tener de suceder repetidas ocasiones o en escalas considerables. La calidad de vida de los habitantes se ve severamente afectada, y con ella, su moral comienza a quebrantarse.

Cabe también mencionar que este tipo de ataques pueden provocar que se cruce la barrera de letalidad que muchos ciber-escépticos argumentan es imposible cruzar por un ente que vive en el mundo digital y no en el físico. Aunque es cierto que el código de computadora por sí mismo no pueda causar letalidad humana, los efectos cinéticos que dicho código pueda generar sí lo pueden hacer.

Volviendo al caso de los sismos en la Ciudad de México, el Instituto Nacional de Psiquiatría advierte que el porcentaje de intentos de suicido entre la población se duplicó tras el sismo de septiembre de 2017 como resultado de TEPT y reconoce que esta catástrofe natural provocó cambios en los estados de ánimo de la población (Mejía, 2017). Este tipo de efectos se desencadenan por asociación una vez que suena la alarma sísmica, convirtiendo su mal uso, como el que le daría un agresor, en un riesgo de seguridad física y mental capaz de causar letalidad humana.

Un ejemplo con potencial de letalidad similar ocurrió en Finlandia en 2016. Un ataque ciber-cinético de Denegación de Servicio Distribuido (DDoS, por sus siglas en inglés) detuvo el sistema de calefacción de dos edificios en la ciudad de Lappeenranta, al este de Finlandia, en pleno invierno (Janita, 2016). El ciber-ataque

desactivó las computadoras que controlaban el sistema de calefacción de los edificios, lo que provocó que, al estar a temperaturas debajo de los 0°C durante el invierno, los residentes tuvieran que ser evacuados y reubicados, sin mencionar los daños materiales causados. Un ataque de esta naturaleza hecho, por ejemplo, durante la noche, cuando la víctima pueda no darse cuenta, puede provocar hipotermias o neumonías que dañen severamente la salud de las víctimas e inclusive lleven a la muerte. Vemos así que incluso en un escenario que no involucre letalidad, la amenaza latente y la afectación a la calidad de vida de las víctimas puede, una vez más, dañar significativamente su integridad física y mental, y con ello, su moral.

FUERZAS ARMADAS

Como centro de gravedad, las fuerzas armadas modernas operan con un arma de doble filo. Desde los años 90s, el ejército de EEUU, tras el cual numerosos países modelan el diseño de sus fuerzas armadas y los conceptos bajo los que operan, adoptó la doctrina militar conocida como Operaciones Centradas en la Red (*Network-centric Warfare*), la cual pretende utilizar redes de computadoras y tecnologías de la información para obtener una ventaja competitiva a través de la superioridad de información en el espacio de batalla.

Los avances tecnológicos del siglo XXI no sólo se aplican a la creación y mejoramiento de nuevas armas, vehículos, aviones o barcos de guerra. Los avances tecnológicos también han revolucionado la manera en que las fuerzas armadas se comunican, coordinan, distribuyen su inteligencia, emiten órdenes, y se reportan con sus comandantes y superiores. Es así que nace la doctrina de Operaciones Centradas en la Red, utilizando redes de computadora, radio e información para ligar prácticamente todos los activos y elementos militares entre sí.

Los beneficios de esta doctrina son significativos: la interconectividad, a través de redes de computadora, entre todos los activos y elementos que utilizan las fuerzas armadas permite tener un conocimiento compartido, en tiempo real, sobre el espacio de batalla completo (tierra, mar, aire, espacio exterior e información), lo cual es aprovechado para obtener superioridad en el dominio de la información y alcanzar los objetivos estratégicos, operacionales y tácticos que se fijen. Inclusive, esta interconectividad y conocimiento compartidos en tiempo real no se limitan exclusivamente a un teatro de operaciones restringido geográficamente, pues con tecnologías satelitales y de largo alcance, la coordinación de las fuerzas armadas puede ocurrir a una escala global (Robb, 2014).

Sin embargo, el doble filo de la doctrina de Operaciones Centradas en la Red, es que el elemento que permite su operatividad y eficiencia, es decir, la red de computadoras e información, es precisamente la misma que la puede hacer vulnerable. En paralelo, la red de computadores e información es el centro de gravedad sin el cual las fuerzas armadas que utilizan la doctrina de Operaciones Centradas en la Red no podrían operar ni coordinarse eficazmente, poniéndolas así en una severa desventaja en el caso de un conflicto armado.

El hecho de que esencialmente todos los activos y elementos militares de una fuerza armada estén conectados entre sí a través de redes de computadoras e información, abre una infinidad de posibilidades para ataques ciber-cinéticos; sin embargo, y para evitar caer en exageraciones o teorías excéntricas, nos limitaremos a aquellas operaciones y proyección de escenarios ciber-cinéticos que ya tienen un precedente real.

Comenzando por los fundamentos, operacionalmente hablando, la doctrina de Operaciones Centradas en la Red hace un amplio uso de satélites en órbita para captar y distribuir información o identificar amenazas. Sin estos satélites, la capacidad de comunicación operacional de una fuerza armada se vería severamente limitada y restringida a zonas geográficas significativamente más pequeñas. Con esto en mente, es seguro afirmar que cualquier fuerza armada que busque aumentar su alcance, coordinación, efectividad y eficiencia operacional utilizando los beneficios de la doctrina de Operaciones Centradas en la Red, tendría que invertir fuertemente en su capacidad satelital.

Es entonces que la ciber-cinética puede jugar un rol en el despliegue de dichas capacidades. A finales de 2017, un cohete ruso que llevaba 19 satélites a bordo con la misión de desplegarlos en órbita sufrió un malfuncionamiento que provocó que el vehículo se desorientara y tuviera un choque fatal con la atmósfera de la Tierra (Berger, 2017). Aparentemente, el sistema de control de vuelo del cohete tenía la configuración equivocada, pues aún estaba programado para despegar desde la base espacial Rusa de Baikonur y no de la nueva base en Vostochny, donde se hizo el lanzamiento.

Este escenario se asemeja a Stuxnet en el hecho de que al infiltrar la red interna de los constructores de los cohetes o de la agencia aeroespacial, sería posible manipular la configuración del objeto físico a través del sistema de computadoras que lo controla. Un ataque ciber-cinético de este tipo y a una escala mayor podría retrasar las capacidades satelitales y, por ende, de comunicación, coordinación y vigilancia militar, de la fuerza armada víctima, sin mencionar los enormes costos que lanzamientos fallidos como éste conllevan.

En un caso similar, en 2015, un transporte militar, el Airbus A400M Atlas, sufrió un mal funcionamiento que lo llevó a estrellarse cerca de Sevilla, España, durante un vuelo de prueba, llevándose consigo no solo al avión sino también la vida de sus cuatro tripulantes (Kelion, 2015). Aparentemente, el accidente fue consecuencia de un error en el software que controlaba los motores del avión. Similar a los PLC que Stuxnet atacó, el avión contaba con un software encargado de interpretar las lecturas de los motores para poder regular la velocidad de los mismos de acuerdo a los comandos de los pilotos, sin embargo, los archivos que dicho software requería para interpretar las lecturas habían sido borrados accidentalmente. Incapaz de interpretar la información viniendo de los motores, el sistema no hizo las modificaciones necesarias para que el avión pudiera mantenerse en el aire, las hélices simplemente giraron más despacio de lo que debían y esto provocó el colapso del avión.

A pesar de que los archivos fueron borrados accidentalmente, una lógica similar a la de los cohetes Rusos o Stuxnet se puede aplicar. Basta que un agente hostil tenga acceso a la computadora del avión para poder manipular procesos o información que provoquen este tipo de incidentes. Los sistemas de vuelo de estos aviones están altamente automatizados, al punto de que los pilotos no pudieron reactivar el sistema de hélices manualmente. Es entonces donde se refleja realmente el alcance e impacto que puede tener el ciberespacio, donde se puede ya incluso afirmar que la seguridad física puede depender de la seguridad digital.

Así como el espacio exterior y el aire presentan vulnerabilidades con potencial de ser explotadas por ataques ciber-cinéticos, el mar y la tierra no se quedan atrás. En 1997, el USS Yorktown de la Marina norteamericana se quedó varado en las costas de Virginia tras sufrir una falla en sus sistemas de navegación ocasionada por el ingreso de información equivocada a la computadora del navío (Slabodkin, 1998). Dicha información equivocada provocó que la base de datos de la computadora se sobresaturara, lo que hizo que fallaran los sistemas de propulsión del navío. El USS Yorktown tuvo que ser remolcado hasta la base naval en Norfolk, Virginia, después de casi tres horas de permanecer inmóvil.

Una vez más, el doble filo de la automatización e interconectividad utilizando redes y sistemas de computadoras es claro. La misma tecnología sobre la cual opera el navío es la misma que lo hace vulnerable. El administrador de los sistemas de control del USS Yorktown cometió el error de ingresar el valor cero en el programa de control, el cual, según los investigadores, no estaba programado para lidiar con el simple error que provoca a la computadora tratar de dividir entre cero, lo que hizo que el sistema se saturara tratando de resolver la anomalía, provocando el colapso de las consolas (Slabodkin, 1998). Un simple número equivocado provocó que un crucero militar de 2,500 toneladas de peso fuera incapaz de moverse por casi tres horas. Las consecuencias operacionales, tácticas e incluso estratégicas que una intrusión ciber-cinética deliberada y hostil de esta naturaleza podría tener en un conflicto armado, o como ataque preventivo, son significativas.

Independientemente de la incapacidad del navío de moverse, las operaciones navales suelen ocurrir en coordinación con otros navíos. El ejemplo más claro son los Grupos de Batalla de Portaviones, formaciones navales en las que el portaviones es escoltado y protegido por un crucero, como el USS Yorktown, un escuadrón de destructores o fragatas y un ala de entre 65 y 70 aviones de combate. Si uno de los navíos que conforman dicho grupo fuera repentinamente incapaz de moverse, la movilidad del grupo entero se vería afectada. Si ese grupo además forma parte de una operación conjunta que involucre otros grupos de ataque, la operación entera podría verse afectada, dependiendo del contexto, la naturaleza de la operación y el nivel de la amenaza.

Los portaviones son los navíos más caros y valiosos de cualquier flota, costando cada uno poco más de $1,000 millones de dólares; por lo que la protección de estas fortalezas flotantes es de suma prioridad. Si uno de los navíos encargados de proteger al portaviones – en este caso el crucero, que es la principal línea de defensa anti-aérea del grupo de combate – es incapaz de moverse, esto pone en alto riesgo al portaviones y al grupo de combate en general.

Cuando se analizan estos escenarios que, aunque hipotéticos, no irrealistas ni imposibles, es que vemos el alcance que un ataque ciber-cinético puede tener y las consecuencias que puede desencadenar.

En tierra se puede desencadenar un efecto similar. Por ejemplo, la artillería en operaciones militares utiliza sistemas de apuntado controlados por computadoras, las cuales son mucho más efectivas y precisas que un humano en el cálculo de los ángulos, velocidad, distancia y altura con que se requiere disparar un proyectil para dar en el blanco. Recientemente, se han desarrollado tecnologías de apuntado automático similares, pero para armas de infantería, como lo son rifles de asalto o de francotiradores. Una de estas tecnologías es TrackingPoint, la cual utiliza un software montado en el arma y que se conecta vía WiFi a una computadora Linux, la cual se encarga de hacer todos los cálculos y ajustes necesarios en la mira del arma para tener una precisión impecable en cada disparo.

El patrón se repite una vez más. La tecnología que amplifica la precisión y eficacia de un arma es la misma que la puede hacer vulnerable. En 2015, los investigadores en seguridad Runa Sandvik y Michael Auger pusieron a prueba la seguridad del sistema TrackingPoint montada en un rifle de francotirador. El resultado de su experimento fue que al utilizar WiFi para comunicar el rifle con la computadora que controla su sistema de apuntado, fue posible explotar vulnerabilidades de seguridad en dicha red y hackear así el arma (Greenberg, 2015a). Una vez dentro del software, los investigadores tuvieron solo que cambiar un valor en el sistema de apuntado automático del rifle para provocar que la bala se desviara casi un metro de distancia de lo que la mira del rifle indicaba. De igual manera, manipulando otras configuraciones del software que controla el rifle fue posible desactivar el sistema de apuntado para provocar que siempre fallara el tiro, o incluso simplemente borrar todos los archivos del programa, provocando que el rifle no pudiera disparar y se volviera prácticamente inútil como arma de fuego.

A pesar de que esta tecnología de apuntado automático en armas de fuego no ha sido aún implementada a gran escala y por ahora se reserva su utilización para fines experimentales o uso exclusivo de las fuerzas especiales, es seguro asumir que una herramienta tal que permita tener 100% de precisión en cada disparo, minimizar el número de municiones requeridas, garantizar tiros críticos y evitar daño colateral, se buscará implementar tarde o temprano en una escala mayor.

Es entonces que con los grandes beneficios de esta tecnología vienen también los grandes riesgos. Vulnerabilidades en los sistemas de apuntado de armas de fuego o artillería puede exponerlas a intrusiones cibernéticas hostiles que inutilicen dichas armas o peor aún, manipulen las miras para atacar blancos distintos a los que el tirador tiene la intención de atacar. Llevado a un extremo, esto puede provocar fuego amigo, es decir, provocar daño a miembros del mismo bando, o incluso fuego no intencional a objetivos neutrales o con quien haya tensiones, como sucede en las zonas militarizadas que vemos hoy en Europa Oriental, el Medio Oriente o la península de Corea, y que pueda provocar el escalamiento de un conflicto.

ECONOMÍA, PRODUCCIÓN Y LOGÍSTICA

Exploraremos los centros de gravedad de economía, producción y logística en conjunto, pues existe una estrecha interrelación entre los tres. La economía se encarga de obtener los recursos y materiales necesarios para sostener la producción suficiente que demande un conflicto armado; la logística se encarga de distribuir dicha producción para asegurar que existan líneas de suministro constantes y eficientes para que la producción llegue a su destino y esté disponible en el momento en que se requiera.

Como demostró el caso de Stuxnet, cada vez son más las industrias cuyos procesos están controlados por sistemas y redes de computadora que los hacen más eficientes. Desafortunadamente, la cultura de "seguridad por obscuridad" ha propagado las vulnerabilidades de estos sistemas, cuyos diseños ignoraron la seguridad de sus redes e interconexiones bajo la creencia de que nadie tendría interés en aprender cómo funcionan sus inusuales programas para tratar de hackearlos y manipularlos.

Hoy en día, las industrias abren cada vez más los ojos a las realidades de las amenazas cibernéticas contra sus sistemas de control y producción. Sin embargo, la Caja de Pandora ya ha sido abierta, por lo que será más una carrera por estar un paso delante de los criminales, grupo o naciones hostiles en términos de ciberseguridad que de eliminar la amenaza por completo. Aceptando esta noción de que la tendencia a atacar sistemas industriales vulnerables continuará, es entonces que la ciber-cinética puede jugar un rol significativo que impacte algunas dinámicas del conflicto armado desde los ámbitos de la economía, producción y logística.

Por el lado económico, el daño que un código de computadora hostil podría ocasionar es severo considerando que las instituciones principales responsables del manejo del dinero, los bancos, dependen casi en su totalidad de poder transferir información a través de redes locales y externas. Los mercados de valores generan todas sus transacciones a través de la red de Internet, donde se mueven cantidades de dinero por billones día tras día. No sólo las grandes empresas y bancos son vulnerables, también lo son los innumerables negocios pequeños que realizan sus cobros y transacciones por Internet y utilizan sistemas de computadora para manejar sus inventarios.

Bajo estas dinámicas se ve claramente que, para la economía, la herramienta tecnológica crucial para poder funcionar es la habilidad de poder transferir información (pagos, transacciones, depósitos, retiros, etc.) entre personas, empresas y bancos. No es de extrañarse entonces que uno de los ataques cibernéticos más grandes de la historia haya atacado precisamente el acceso a los sistemas de computadora y a la información contenida en ellos. En mayo de 2017, más de 230,000 computadoras de más de 100,000 instituciones en más de 150 países fueron infiltradas por un criptogusano conocido como *WannaCry,* en lo que se convirtió en el ataque de *ransomware* más grande jamás visto.

WannaCry fue básicamente un ataque de extorsión. Una vez infiltradas las computadoras, el gusano se encargaba de encriptar, total o parcialmente, los archivos y el acceso a las computadoras infectadas. Si la víctima deseaba recuperar acceso a su sistema y a su información, debía pagar un rescate utilizando la criptomoneda Bitcoin. Un mes después del inicio de los ataques, se habían ya hecho 327 pagos de rescate que sumaron un total de $130,634.77 USD (51.62396539 Bitcoins) ("@actual_ransom tweets", 2017). La firma de riesgos cibernéticos Cyence estimó que los daños que *WannaCry* provocó alcanzaron los $4,000 millones de dólares (Berr, 2017).

Entre las instituciones más afectadas se encontraron el Servicio Nacional de Salud Británico, universidades, empresas de comunicación como “Telefónica” de España y “Saudi Telecom” de Arabia Saudita, varias instituciones gubernamentales y algunos bancos. A diferencia de Stuxnet, *WannaCry* no tenía un objetivo en específico y simplemente buscaba infectar a tantas computadoras como le fuese posible. Lo alarmante de este factor es que, a pesar de no haber sido un ataque dirigido a un objetivo específico en el que se conocen todas las características técnicas del mismo, aun así, fue capaz de infectar cientos de miles de valiosos sistemas de computadoras, lo cual refleja la epidemia de inseguridad que hay en el mundo cibernético, incluso en instituciones e industrias consideradas críticas para la economía y seguridad nacional de los países.

Considerando que, durante un conflicto armado, o en el preámbulo de uno, la mayoría de grupos o naciones se movilizan hacia lo que se conoce como “Economía de Guerra”, en la que se busca organizar y distribuir la economía y producción de un grupo o nación para priorizar el esfuerzo de la guerra y cubrir las necesidades básicas de los consumidores, ciberataques de la naturaleza de *WannaCry* podrían causar daño significativo al flujo de dicha economía. Escenarios como congelamiento o robo de cuentas bancarias, desvío de fondos o bloqueo de acceso a cuentas o sistemas de información podría poner una enorme presión sobre el flujo cotidiano de la economía, obligando a instituciones y usuarios a remitirse a métodos más rudimentarios y menos eficaces para mantener activa la economía y servicios.

Así como un ataque cibernético podría poner en serios apuros los sistemas financieros de un grupo o nación, la amenaza es similar para los medios de producción y distribución, los cuales son componentes esenciales

de una economía de guerra. Como se mencionó anteriormente, la gran mayoría de los países industrializados cuentan con producciones y manufacturas a gran escala y que son operadas hoy en día por máquinas y robots encargados de construir vehículos, partes y refacciones, alimentos empaquetados, medicinas y hasta servicios públicos esenciales.

Cabe mencionar que la industria de la maquinaria y robots de producción industrial tiene estrictos estándares, por lo que la arquitectura de la mayoría de las máquinas y robots industriales modernos es muy similar (Maggi, 2017). A pesar de que esto estandariza y optimiza las operaciones cotidianas de las industrias, al mismo tiempo provoca que si uno de sus elementos es vulnerable, todos puedan ser vulnerables por extensión dada la similitud entre ellos. En 2017, la empresa de ciberseguridad Trend Micro se dio a la tarea de poner a prueba las máquinas y robots de producción más comunes utilizadas por distintas industrias para evaluar su vulnerabilidad a ataques cibernéticos. Los resultados no fueron prometedores.

El resultado del experimento fue que la mayoría de las máquinas y robots de producción funcionan utilizando softwares obsoletos, el cual usa sistemas operativos y librerías de archivos vulnerables y antiguas. Inclusive, el equipo de investigación encontró que muchas máquinas y robots industriales utilizan direcciones de Protocolo de Internet (IP por sus siglas en inglés y cuya función es el envío de paquetes de información tanto a nivel local como a redes externas) públicas, lo que las hace vulnerables a ataques remotos (Maggi, 2017).

En total, el equipo de investigación identificó cinco diferentes tipos de ataques cibernéticos con efectos cinéticos capaces de afectar el nivel de seguridad, precisión e integridad con el que operan las máquinas y robots de producción industrial.

Dos de dichos tipos de ataques involucran la manipulación de la información sobre el estatus de la máquina o robot en operación. Esta manipulación puede poner en alto riesgo a los operadores de las máquinas o robots. En uno de los escenarios, el sistema fue manipulado para reportar al operador que los motores estaban apagados o que la máquina o robot estaba operando bajo condiciones normales. Si el operador, confiado de que las medidas de seguridad son las correctas, se acerca a continuar operando la máquina, puede sufrir grave daño físico, incluso mortal. En un escenario hostil, independientemente del daño causado a algún operador individual, el verdadero daño es el miedo y paranoia colectiva que un ataque de esta naturaleza podría generar en toda una planta o industria que esté siendo blanco de ataques ciber-cinéticos. Sin poder garantizar la seguridad de los operadores, es posible que se rehúsen a seguir trabajando y la producción decaiga a un alto total.

Los otros tres tipos de ataques involucran la manipulación de los parámetros de control o de calibración de las máquinas o robots. El resultado de estas manipulaciones es, en primer lugar, daños parciales o totales a las máquinas o robots, lo cual conllevaría costos extras para su reparación o reemplazo y, sobre todo,

retrasaría la capacidad de producción; en segundo lugar, las manipulaciones pueden generar una producción defectuosa del producto en construcción. Un cambio en los parámetros de control puede provocar que, por ejemplo, la alineación de la máquina o robot se altere por algunos milímetros, una medida difícil de identificar a la vista pero que puede provocar malfuncionamientos severos en el producto final.

Durante sus experimentos, los investigadores comprobaron cómo dicho defecto de tan solo 2 milímetros en la hélice de un dron provocó que éste fallara a la hora de volar y colapsara al suelo. En un escenario hostil, un ataque ciber-cinético de esta naturaleza a gran escala podría ocasionar que una enorme cantidad de productos, vehículos, partes o refacciones contengan defectos de fabricación que son prácticamente invisibles a la vista humana y que no serán evidentes hasta que ocurra el malfuncionamiento del objeto. Las consecuencias de esto serían incómodas, pues implicaría más inversión de recursos en la reparación de objetos defectuosos, además de retrasar o inhabilitar la logística para la que fueron construidos originalmente; y que, si estamos hablando de un conflicto armado, donde la puntualidad en la disponibilidad de armamento o vehículos es crucial, puede provocar una reacción en cadena similar a la analizada en el caso del USS Yorktown del subtítulo anterior.

No sólo es la producción industrial que se puede ver afectada por ataques cibernéticos, incluso las propias materias primas necesarias para dicha producción industrial pueden estar en riesgo. En 2015, la Oficina Federal de Seguridad de la Información Alemana reportó daños masivos a un molino de acero alemán provocado por un ataque ciber-cinético de naturaleza similar a Stuxnet. El ataque cibernético tuvo como objetivo los sistemas de control de los altos hornos, los cuales fueron manipulados y provocaron que no pudieran ser apagados y cerrados apropiadamente, causando así un daño masivo a la planta en general (Zetter, 2015).

Aparentemente, los hackers obtuvieron acceso a los sistemas de control industriales a través de la red de negocios de la planta, la cual lograron infiltrar inicialmente utilizando un sencillo ataque de *spear-fishing*, el cual consiste en enviar un correo electrónico que aparentemente viene de una empresa reconocida y confiable como Google o PayPal y que, al momento de ser abierto, descarga en la computadora de la víctima el código malicioso que infiltra la red interna.

Algo curioso de este ataque es que aún no es claro si el objetivo de los hackers era el de causar daño físico a las instalaciones de la planta. Tras la infiltración inicial, los hackers simplemente se dedicaron a explorar la red interna de la planta, y en el proceso, dañaron algunas configuraciones y sistemas que eventualmente llevaron a la falla de los sistemas de control industriales que provocaron el incidente con los altos hornos. Lo que esto sugiere es que existe una posibilidad de que el daño cinético causado a la planta haya sido mero daño colateral, lo cual puede hacer este tipo de ataques aún más peligrosos pues – a diferencia de un código como Stuxnet, con objetivos y funciones perfectamente definidas – un código malicioso sin dicha precisión

puede incluso salirse del control de sus diseñadores y causar efectos colaterales no previstos ni intencionados.

En un escenario de conflicto armado, un ataque cibernético de esta naturaleza puede afectar no solo la producción interna de algún grupo o nación, sino también la economía de aquellos actores para quienes la exportación de materias primas y recursos naturales es una actividad económica primordial, como es el caso del petróleo en países de Oriente Medio o el de energía en Rusia.

ÉLITES POLÍTICAS O MILITARES

A pesar de la predominancia de los gobiernos democráticos en la mayoría de los países Occidentales, es difícil argumentar contra el hecho de que la política interna de los países, así como las relaciones internacionales, son comúnmente orquestadas por élites políticas o militares, y en algunos casos, por un individuo con poder cuasi absoluto.

La historia está repleta de ejemplos, desde el mundo de Alejandro Magno, el imperio de Constantino o las hordas de Gengis Kan hasta la Francia de Napoleón, la Alemania de Hitler o los EEUU de J. F. Kennedy, existen aún hoy en día líderes que, ya sea gobiernen de manera democrática o autoritaria, tienen proyectos e ideologías de nación que definen la realidad de dicha nación y de aquellas comunidades o países sobre los que tienen influencia. Independientemente del juicio que se le pueda hacer a los proyectos e ideologías de cada líder, el factor clave para este análisis es el entendimiento de que, al ser estos líderes las mentes maestras detrás de sus planes y visiones, esto los convierte en el centro de gravedad de los mismos; sin su liderazgo, es difícil pensar que sus proyectos e ideologías puedan continuar intactos.

Identificando este centro de gravedad es que comienzan a abrirse las posibilidades para aquellos individuos, grupos o naciones que estén en contra de las políticas o proyectos de algún líder o élites políticas o militares y busque tomar acción hostil contra ellos. Increíblemente, la ciber-cinética ya ha demostrado que, bajo escenarios específicos, es una herramienta capaz de lograr dicho objetivo.

Como analogía, consideremos que, tras una investigación de una década, finalmente se determinó que el incidente automovilístico en el que falleció la Princesa Diana de Gales en 1997 fue una matanza ilegal y no un mero accidente. El choque que provocó el fallecimiento de Diana se debió a la negligencia del chofer, Henri Paul, quien comenzó a conducir de manera peligrosa y desconsiderada para tratar de evadir a un paparazzi que perseguía a la Princesa de Gales. A pesar de que en el caso de Diana el choque fue causado por negligencia humana, las nuevas generaciones de automóviles – que prácticamente en su totalidad contienen computadoras integradas y más recientemente, acceso a Internet para sus sistemas de navegación y entretenimiento – pueden ser vulnerables a ataques ciber-cinéticos con consecuencias similares a las que sufrió la Princesa Diana.

En 2015, los investigadores en seguridad cibernética Charlie Miller y Chris Valasek demostraron la vulnerabilidad de varias compañías automovilísticas y la capacidad de un potencial hacker hostil de acceder a la computadora del vehículo remotamente utilizando la conexión de Internet del mismo (Greenberg, 2015b). En su experimento, Charlie y Chris infiltraron la computadora de una Jeep Cherokee a través de *Uconnect*, el sistema de entretenimiento de la camioneta, mientras ésta era conducida por un asistente del experimento. Una vez hackeado, y desde la comodidad de su sala, los investigadores comenzaron por activar los sistemas de aire acondicionado y de sonido del vehículo; después, activaron los limpiaparabrisas, lo cual comenzó a dificultar la visibilidad del conductor. Finalmente, Charlie y Chris apagaron remotamente el motor del vehículo, el cual quedó varado en medio de una autopista de alta velocidad. Cabe mencionar que el vehículo, al estar bajo control remoto de los hackers, no respondía a ninguna acción manual que el conductor intentaba llevar a cabo.

Sin embargo, el arsenal de opciones disponibles para un agresor que pretenda hacer daño a una víctima viajando en automóvil va más allá de lo que los investigadores demostraron en su experimento inicial. Siguiendo el mismo procedimiento, es también posible modificar la velocidad de tránsito del vehículo, activar los frenos abruptamente, deshabilitarlos en su totalidad, y hasta maniobrar el volante del automóvil remotamente. Inmediatamente se vuelven evidentes las consecuencias que un ataque cibernético de esta naturaleza puede tener si un grupo o nación hostil lograse tomar control remoto del vehículo de su víctima, que bien puede ser un líder o miembro de la élite política o militar, como fue el caso de la Princesa Diana de Gales.

Similar a como sucede con los sistemas de control industriales, los diseñadores de los programas y redes de computadora que utilizan los automóviles modernos no han hecho la seguridad de dichos sistemas una prioridad, en parte por la similar lógica de “seguridad por obscuridad” que, por ejemplo, asume que nadie tendría interés en infiltrar el sistema de entretenimiento de un automóvil. Hasta cierto punto se puede perdonar esta ingenuidad bajo el hecho de que ataques cibernéticos como los que demostraron Charile y Chris no tienen prácticamente ningún precedente. Sin embargo, una vez abierta la Caja de Pandora, no hay vuelta atrás y la seguridad de los sistemas de computadora y redes de los automóviles tendrán que ser tomados más en serio.

Así como es comprensible que, a primera vista, sea difícil pensar que los sistemas de navegación o entretenimiento de un automóvil puedan representar un riesgo de seguridad, hay otro objeto en particular del cual se podría decir lo mismo. La tecnología ha permitido que los tradicionales marcapasos y desfibriladores implantables contengan ahora sistemas de comunicación inalámbricas que permitan al programador o al doctor a cargo de un paciente hacer ajustes, recolectar información y llevar a cabo procesos y tratamientos médicos remotamente y sin necesidad de una cirugía médica.

A pesar de la enorme practicidad que dicho sistema permite, la conexión inalámbrica que posee lo hace vulnerable a intrusiones cibernéticas, especialmente considerando que, como los sistemas de control industrial o los sistemas de navegación y entretenimiento de un automóvil, la seguridad digital de los marcapasos y desfibriladores implantables no es usualmente una prioridad o siquiera una consideración de sus diseñadores.

En 2008, investigadores de seguridad de la Escuela Médica de la Universidad de Harvard advirtieron por primera vez de la vulnerabilidad de los desfibriladores implantables y las devastadoras consecuencias que podría tener el hackeo de dichos aparatos (Applegate, 2013, p. 4). Los investigadores demostraron que utilizando una simple laptop era posible interceptar la conexión inalámbrica del desfibrilador y acceder a su sistema de control utilizando un nombre de usuario no encriptado y una contraseña que por lo general era el número de serie del aparato. Una vez dentro, el hacker podía manipular las funciones del objeto o extraer información del mismo, desde el nombre y fecha de nacimiento del paciente, hasta su historial médico.

A pesar de las recomendaciones hechas en 2008 para mejorar la seguridad de estos aparatos, en 2012, el investigador en seguridad Barnaby Jack demostró lo vulnerable que aún eran las conexiones inalámbricas de los marcapasos y desfibriladores. En su demostración, Barnaby hackeó un marcapasos y, utilizando comandos en su computadora, envió una descarga de 830 voltios al aparato, suficientes para provocar daño severo o mortal a la víctima. De igual manera, Barnaby demostró la capacidad de provocar un infarto al corazón utilizando comandos de computadora o incluso deshabilitar las instrucciones de respuesta del aparato en caso de alguna emergencia (Applegate, 2013, p. 5).

Al igual que con la vulnerabilidad de los sistemas de control de automóviles, una persona de interés con implantes médicos vulnerables correría un serio peligro si se convirtiera en objetivo de un grupo o nación hostil. La lista de candidatos contiene nombres lo suficientemente relevantes como para considerar seriamente esta amenaza. Basta una búsqueda en Internet para descubrir que personajes como Carlo Azeglio Ciampi, ex-presidente de Italia; Gerald Ford, ex-presidente de los EEUU; Dick Cheney, ex-vicepresidente de los EEUU; o el Papa Benedicto XVI, líder de la Iglesia Católica, utilizaron o aún utilizan marcapasos implantados.

EN PERSPECTIVA

Para finalizar este análisis, es importante poner los hallazgos y escenarios aquí expuestos en perspectiva. A primera vista, puede ser tentador calificar este análisis como alarmista o exagerado; por lo que, con el propósito de mantener una objetividad en el análisis, es necesario mencionar y elaborar sobre los factores y contextos que acompañan los fenómenos ya analizados.

Primeramente, cabe recordar que los escenarios hipotéticos expuestos en este análisis tienen un precedente real, mencionado y citado en cada caso particular; no se trata de una especulación sin fundamentos. Lo que se tiene que entender es que el fenómeno de los ataques cibernéticos y la ciber-cinética son, como ya se ha mencionado, una Caja de Pandora que, una vez abierta, se limita solo a la imaginación, creatividad y capacidad del individuo, grupo o nación que pretenda utilizarlos. Este análisis se limitó a explorar el potencial que los ataques cibernéticos pueden tener, fundados en precedentes reales, en los centros de gravedad de escenarios de conflictos armados o en el preámbulo de éstos; sin embargo, su alcance es prácticamente tan grande como la proporción en la que nuestra vida cotidiana y sus procesos estén cada vez más conectados a sistemas y redes de computadoras.

Para poner el rol de las operaciones cibernéticas en perspectiva, es importante considerar dos de los atributos más característicos del ciberespacio y que lo hacen una atractiva alternativa a las dinámicas tradicionales bajo las que se lleva a cabo un conflicto armado o el preámbulo del mismo. Como primer atributo, y asumiendo que el objetivo puede ser alcanzado cibernéticamente, los ataques cibernéticos son generalmente más eficientes que una operación militar convencional, pues, por un lado, los costos de operaciones cibernéticas son menores, y por el otro, no se ponen en riesgo vidas humanas, al menos no del bando del agresor. Aunado a esto, hay que considerar que los ataques cibernéticos no tienen las limitaciones geográficas que los ataques convencionales sí tienen, el código de computadora puede viajar a través de redes instantáneamente y a cualquier lugar del planeta donde exista la infraestructura necesaria.

Como segundo atributo, las operaciones cibernéticas tienen un alto grado de negación plausible, es decir, existe un problema de atribución que permite a un agresor ocultar su identidad si así éste lo desea. Esto permite que el costo político de llevar a cabo un ataque cibernético pueda ser muy bajo o incluso nulo. La explicación de dicho problema de atribución es meramente técnica, pues los orígenes de un ataque o los servidores donde se hospedan los archivos maliciosos pueden ser mal dirigidos por el perpetrador. Por ejemplo, uno de los servidores que hospedaba los archivos de Stuxnet estaba localizado en Dinamarca; sin embargo, sabemos que Dinamarca no tuvo ningún involucramiento en la perpetuación del ataque.

Como consecuencia del problema de atribución es que un grupo o nación puede llevar a cabo una operación cibernética hostil con un bajo riesgo de que la situación escale al nivel de un conflicto armado convencional, tal y como sucedió con las operaciones cibernéticas y electrónicas que Rusia llevó a cabo durante sus operaciones en Crimea, la cual logró anexar sin escalar a un conflicto armado con la OTAN. A este tipo de conflictos se les conoce como guerras híbridas, pues combinan elementos físicos y digitales o electrónicos para alcanzar sus objetivos. El gran reto de este tipo de guerras es el de definir dónde está la línea bajo la cual una operación hostil ya se considera un acto de guerra o no, lo cual es difícil de lograr cuando no se

tiene certeza o evidencia contundente de quién es el responsable de un ataque, gracias a la negación plausible que permiten las operaciones cibernéticas.

El problema de atribución se resuelve parcialmente más por contexto que por evidencia tangible. Por ejemplo, aunque no haya evidencia directa que ligue a Stuxnet con quien haya sido su creador, la realidad es que un código tan complejo y una operación tan meticulosa sólo pudieron ser perpetrados por una nación con grandes capacidades cibernéticas, con una efectiva red de inteligencia, y con amplios recursos para invertir en dicho proyecto. Una vez consideradas estas variables, la lista de posibles responsables se vuelve muy específica. Si además se consideran intereses o rivalidades políticas, todo apunta a que fue una operación realizada por los EEUU y su aliado Israel.

Considerando estos dos atributos del ciberespacio es que es posible sugerir que la mayor utilidad y aplicación de las operaciones cibernéticas, específicamente de los ataques ciber-cinéticos, se da durante conflictos preventivos cuyos objetivos son los de disuadir a un posible agresor, obtener una ventaja estratégica antes de comenzar un conflicto armado inminente, o prevenir que un enemigo adquiera o mantenga capacidades, principalmente militares, que puedan ser utilizadas de forma hostil. El ataque de Japón a Pearl Harbor durante la Segunda Guerra Mundial, así como la invasión de EEUU a Irak en 2003, son ejemplos clásicos de guerras preventivas. Stuxnet es el mejor ejemplo actual que ilustra dicha dinámica, pues a través de un ataque ciber-cinético se buscó eliminar o al menos retrasar la adquisición de capacidades nucleares por parte de Irán.

A una guerra preventiva se le considera una guerra limitada, que, a diferencia de una guerra total, utiliza solo algunos elementos de poder y tiene objetivos específicos y limitados que no involucran la destrucción total o rendición incondicional del enemigo. Es en este tipo de conflictos “pasivos” que las operaciones ciber-cinéticas pueden ser de mayor utilidad, pues permiten alcanzar objetivos o “pequeñas victorias” a bajo costo, sin poner en riesgo vidas humanas aliadas y con la posibilidad de deslindarse de la responsabilidad del ataque, lo cual es una propuesta muy atractiva para cualquier grupo o nación, especialmente si ésta no cuenta con capacidades militares suficientes para coercer o disuadir a su rival en un conflicto convencional.

Utilizando el juego de ajedrez como analogía, un ataque ciber-cinético en una guerra preventiva o limitada, o en el preámbulo de la misma, sería el equivalente a utilizar alguna táctica que permita obtener una ventaja posicional o de material durante la partida de ajedrez, incluso la mínima ventaja, como sería la captura de un peón sin perder una pieza propia en respuesta o la colocación de una pieza poderosa en una casilla dominante en el tablero. En dicho escenario, a pesar de que el jugador rival es capaz de seguir jugando la partida, se encuentra ya en una desventaja que sólo se hará más grande conforme más piezas se vayan intercambiando entre ambos jugadores. Es por esto que, a nivel profesional, donde difícilmente los jugadores cometen errores graves, es común que el jugador que se encuentra en desventaja se rinda incluso si aún no está en una situación de jaque mate, pues entiende que está en una posición desventajosa de la que

difícilmente podrá recuperarse y entonces decide no seguir gastando sus esfuerzos y energías en una partida que está prácticamente perdida.

Esta analogía ilustra cómo a pesar de que un ataque ciber-cinético pueda no otorgar una victoria decisiva por sí mismo, sí puede desencadenar un efecto que, de continuar o de sumarse a otras ventajas, cibernéticas o no, pondría al rival en una posición desventajosa, disuadiéndolo así de continuar gastando sus recursos en una causa difícil de ganar. Cabe mencionar una vez más que la manera en que se puedan o no desencadenar los efectos que busca lograr un ataque cibernético es subjetivo a la escala, capacidades y contexto tanto de los actores involucrados como del conflicto en cuestión. Las capacidades de un país como México son muy distintas a las capacidades de potencias militares como EEUU, Rusia, China o Corea del Norte; igualmente, los contextos de un conflicto como la guerra de Corea o Vietnam, donde se buscaba frenar la expansión del Comunismo Ruso, es distinto a una guerra de conquista o aniquilación donde la propia supervivencia del atacado está en juego, por lo que su tolerancia al daño que considere inaceptable será mucho más alta.

Hablando de las capacidades que posea o no un grupo o nación con intención de llevar acabo algún ataque cibernético, es importante entender que dichos ataques difícilmente suceden de manera aislada y más bien requieren de una efectiva red de inteligencia que guíe sus pasos. La prominencia de los ataques cibernéticos, así como el bajo costo y relativa facilidad con que se pueden llevar a cabo – si se comparan con la complejidad de un ataque convencional – ha creado la popular percepción de que cualquier adolescente con una laptop y conexión a Internet puede perpetuar un ataque cibernético desde el sótano de su casa.

Aunque sí es cierto que prácticamente cualquier persona con suficientes habilidades para programar un código malicioso y esparcirlo por el Internet es capaz de perpetuar un ataque cibernético, el tipo de ataques que estas personas realizan se consideran más bien ciber-crímenes de una escala e impacto menor a los que hemos cubierto en este análisis y que difícilmente se podría argumentar que tengan un impacto en las dinámicas de la guerra moderna. La realidad es que, para ejecutar exitosamente un ataque de impacto considerable, como Stuxnet, se necesita no solo contar con la capacidad técnica para diseñar y desplegar el código malicioso, sino una capacidad de inteligencia que proporcione toda la información necesaria para que el ataque sea exitoso.

¿Cómo sabrían los diseñadores de Stuxnet la compañía y el modelo específico que utilizaban los microchips que controlaban los centrifugadores de la planta? ¿Cómo sabrían exactamente el rango de velocidad al que rotaban los motores de los centrifugadores que Stuxnet buscaba? ¿Cómo conocerían la contraseña secreta que se requería para que Stuxnet hackeara el programa *Step 7* instalado en los sistemas de control industrial de la planta? Preguntas como éstas no pueden ser respondidas ni mucho menos utilizadas en el diseño de un ataque cibernético si no existe un aparato de inteligencia que proporcione dicha información. Por esta

razón, un ataque cibernético del calibre de Stuxnet es tan una operación cibernética como es una operación de espionaje e inteligencia.

Un ejemplo ideal para ilustrar la estrecha relación entre un ataque cibernético y la inteligencia es el espionaje industrial y militar que realiza China. Los EEUU saben que el Ejército de Liberación Popular Chino tiene una unidad de espionaje cibernético que ha sido responsable en gran medida del robo de inteligencia y tecnología militar estadounidense. Si alguna vez alguien se pregunta por qué los aviones de combate chinos se parecen tanto a los aviones de combate estadounidenses, la razón es porque China ha robado algunos de los planos de dichos aviones para construir los suyos.

Sin embargo, los EEUU, bajo el conocimiento de que algunos planos de sus aviones de combate estaban siendo robados, comenzaron una operación de contraespionaje en la que intencionalmente subió a su red militar planos de aviones de combate que contenían algunos errores en su diseño o programación. La idea era que China, al robar dichos planos, construyera aviones de combate con diseños defectuosos o con vulnerabilidades cibernéticas. De tener éxito, un avión chino construido con alguna de estas vulnerabilidades cibernéticas, permitiría a los EEUU acceder remotamente a los sistemas de control del avión y poder manipular varias de sus funciones e inutilizar así el avión, y por extensión, todos aquellos aviones de combate chinos construidos siguiendo planos estadounidenses robados y defectuosos o manipulados.

Sin un aparato de inteligencia, y en este ejemplo, de contrainteligencia, los EEUU no tendrían la información necesaria para poder llevar a cabo operaciones cibernéticas que respondieran al robo de su tecnología militar por parte de China. Dada la estrecha relación entre las operaciones cibernéticas y la inteligencia, se puede argumentar que la seguridad cibernética comienza con la seguridad de la información. La capacidad de contrainteligencia y contraespionaje que posea un grupo o nación va a tener un impacto directamente proporcional en su ciberseguridad.

Es importante reconocer esta relación, pues en términos de crear políticas o legislación para fortalecer la ciberseguridad de un grupo o nación, sería un grave error aislar dicha seguridad cibernética y no buscar fortalecer también al aparato de inteligencia y contrainteligencia que facilite o dificulte la ejecución de un ataque cibernético de escala y efectos serios y relevantes.

Finalmente, hay que entender que las operaciones cibernéticas, como un ataque ciber-cinético, difícilmente van a tener un efecto coercitivo o disuasivo decisivo por sí mismas; sin embargo, el valor del ciberespacio es que, como se analizó en los escenarios presentados, ofrece opciones y posibilidades costo-efectivas, de bajo riesgo y altamente accesibles, en comparación con sus contrapartes físicas convencionales, no antes disponibles como elementos de poder. Al final del día, la coerción o disuasión de un rival comúnmente

requiere una orquestación de distintos elementos de poder en todos los dominios (tierra, aire, mar, espacio e información) de manera que se apoyen y complementen mutuamente.

Es en ese dinamismo por alcanzar objetivos o agendas políticas a través del uso de los elementos de poder disponibles para un grupo o nación donde el ciberespacio encaja y encuentra su papel. Desde la enorme paleta de opciones que presenta el mundo cada vez más interconectado – y como se vio en este análisis, vulnerable – en el que vivimos, hasta la negación plausible que puede tener un ataque cibernético, es difícil pensar que la tendencia actual y futura para grupos o naciones que busquen proteger su seguridad nacional, mejorar su defensa, o avanzar sus agendas políticas, no incluya un fuerte componente de actividad cibernética.

CONCLUSIÓN

La guerra es siempre un producto de su época. Las herramientas, estrategias y tácticas que el ser humano ha utilizado para hacer la guerra siempre han evolucionado junto con su tecnología. Este es un patrón que continua hasta el día de hoy. La guerra en la Era de la Información actual inevitablemente tendrá características que la distinguirán de las eras previas. Dichas características afectan las capacidades que se utilizan en los tres niveles del conflicto (estratégico, operacional y táctico) así como la naturaleza del ambiente en el que los conflictos ocurren.

Uno de los ambientes que ha traído consigo la Era de la Información es el ciberespacio, cuya noción comúnmente asume, erróneamente, que, al ser un ente digital, no tiene repercusión alguna en el mundo físico. Sin embargo, fenómenos como la ciber-cinética han demostrado en varias ocasiones la capacidad de utilizar código de computadora con intenciones hostiles y con la facultad de tener efectos cinéticos con consecuencias físicas y tangibles en el "mundo real".

El mejor y más relevante ejemplo es el ataque ciber-cinético de Stuxnet a la planta de enriquecimiento de uranio en Natanz, Irán. Independientemente del daño limitado que el ataque haya causado, la importancia es que el ataque dejó ya un precedente que abrió la Caja de Pandora de los ataques ciber-cinéticos. El simple hecho de haber demostrado lo que es posible hacer y el daño que es posible causar a través de un código de computadora, marcan un parteaguas en las dinámicas y conceptualización de los conflictos armados y del que sin duda alguna apenas estamos descubriendo la superficie.

Asumiendo que se cuenta con el conocimiento técnico y los recursos para montar un ataque ciber-cinético a gran escala o de alto impacto, existen ya precedentes históricos que pueden ser directamente desplegados contra los centros de gravedad de un grupo o nación. Estos centros de gravedad son elementos críticos, de balance, sin los cuales la estructura completa de un grupo o nación podría colapsar. Utilizando ataques ciber-cinéticos, es posible quebrantar sistemáticamente la resistencia de uno o varios centros de gravedad, ya sea

parcial o totalmente. Es importante tener en cuenta que un ataque cibernético difícilmente podría tener un efecto decisivo por sí mismo en un conflicto armado o en el preámbulo de uno. El ciberespacio forma parte de un espacio de batalla en el que también operan los dominios del mar, aire, espacio exterior y sobre todo el terrestre, el dominio más importante de todos pues es donde habita el ser humano.

Es importante considerar también que el simple hecho de conocer la existencia y alcances de un ataque cibernético no significa que cualquier grupo o nación pueda llevar a cabo un ataque de dicha naturaleza, al menos no en una escala que contribuya a generar daño inaceptable para coercer o disuadir a un enemigo. Las capacidades y conocimiento técnico, los recursos disponibles, y, sobre todo, un aparato de inteligencia y espionaje que proporcione la información necesaria y relevante para diseñar un ataque cibernético son cruciales para el éxito del mismo. Naturalmente, el número de grupos o naciones que cuentan con dichas capacidades y recursos hoy en día es limitado, pero podemos estar seguros, con alto nivel de confianza, que las capacidades cibernéticas serán una prioridad en las agendas y presupuestos de todo aquél grupo o nación que busque optimizar su seguridad o avanzar su agenda política a un costo económico y político aceptable, especialmente si no se cuenta con las capacidades convencionales de una potencia militar que le permita coercer o disuadir en favor de sus intereses.

Dada la naturaleza de los ataques cibernéticos aquí analizada, es evidente que la accesibilidad para ejercer presión coercitiva sobre algún rival ha bajado considerablemente, es decir, grupos o naciones cuyas capacidades militares jamás les habrían permitido ejercer presión coercitiva o amenazar con acción hostil capaz de disuadir a algún rival para alcanzar objetivos políticos, tienen ahora una herramienta que les puede permitir cierta latitud de acción. Es así que, con un aumento en el número de actores con opciones cibernéticas capaces de ejercer presión coercitiva o disuasiva, la máxima de Vegecio – s*i vis pacem, para bellum* (si quieres la paz, prepárate para la guerra) – es más relevante ahora que nunca para cualquier grupo o nación que busque salvaguardar su seguridad nacional y mantenerse relevante en estas nuevas dinámicas cibernéticas que le permitan avanzar su agenda e intereses.

BIBLIOGRAFÍA

"@actual_ransom tweets", Twitter

Albright, D., Paul Brannan and Christina Walrond. (2010). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?.* Institute for Science and International Security

Applegate, S. D. (2013). *The Dawn of Kinetic Cyber.* NATO CCD COE Publications, Tallinn

Banerjee, S. (2017). *Independent Defense Coordination - Defense Negotiation Tools and Tackles*. Sabyasachi Banerjee Independent Consultants and Industrial Mentor and Planning

Berger, E. (2017, Noviembre 30). *This week's failed Russian rocket had a pretty bad programming error*. https://arstechnica.com/science/2017/11/this-weeks-failed-russian-rocket-had-a-pretty-bad-programming-error

Berr, J. (2017, Mayo 16). *"WannaCry" ransomware attack losses could reach $4 billion*. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses

Clausewitz, C. (1993). *On War*. Translated by Michael Howard and Peter Paret. New York, Knopf

Cybint. (2017, Septiembre 26). *The Scary Truth About Cyber Security*. https://www.cybintsolutions.com/cyber-security-facts-stats

Federal Bureau of Investigation. (2017). *How to Protect Your Networks from Ransomware: Technical Guidance Document.* US Government

Foster, H. (2017, Octubre 5). *The Air Domain and the Challenges of Modern Air Warfare*. https://www.heritage.org/military-strength/the-air-domain-and-the-challenges-modern-air-warfare

Greenberg, A. (2015a, Septiembre 29). *Hackers Can Disable A Sniper Rifle – Or Change Its Target*. https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target

Greenberg, A. (2015b, Julio 21). *Hacker Remotely Kill A Jeep On The Highway – With Me On It.* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

Ivezic, M. (2017a, Mayo 20). *Timeline of Key Cyber-Kinetic Attacks, Incidents and Research.* http://ivezic.com/cyber-kinetic-security/timeline-key-cyber-kinetic-attacks-incidents-research

Ivezic, M. (2017b, Diciembre 15). *Our smart future and the threat of cyber-kinetic attacks.* https://www.helpnetsecurity.com/2017/12/15/cyber-kinetic-attacks

Ivezic, M. (2018, Enero 2). *The tangible threat of cyber-kinetic attacks*. https://www.csoonline.com/article/3245036/cyberwarfare/the-tangible-threat-of-cyber-kinetic-attacks.html

Janita (2016, Noviembre 7). *DDoS attack halts heating in Finland amidst winter.* http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

Keizer, G. (2010, Septiembre 16). *Is Stuxnet the 'best' malware ever?*. https://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html

Kelion, L. (2015, Junio 10). *Fatal A400M crash linked to data-wipe mistake*. http://www.bbc.com/news/technology-33078767

Maggi, F. (2017, Mayo 3). *Rogue Robots - Testing the Limits of an Industrial Robot's Security*. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security

Mejía, X. (2017, Septiembre 22). *¿Cómo enfrentar el estrés postraumático y un potencial suicidio?*. http://www.excelsior.com.mx/comunidad/2017/09/22/1190121

Musa, S. (2014, Marzo). *Advanced Persistent Threat – APT.* University of Maryland University College, Computer Networks and Cyberscurity. https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT

Nakashima, E. and Joby Warrick (2012, Junio 2). *Stuxnet was work of U.S. and Israeli experts, officials say*. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.dca1ea078bb1

Newman, L. H. (2017, Abril 10). *That Dallas Siren Hack Wasn't Novel – It Was Just Really Loud.* https://www.wired.com/2017/04/dallas-siren-hack-wasnt-novel-just-really-loud

Pollpeter, K. (2012). *Controlling the Information Domain: Space, Cyber, and Electronic Warfare*. The National Bureau of Asian Research

Rid, T. and Peter McBurney. (2012). *Cyber-Weapons*. The RUSI Journal. Vol. 157. No. 1. pp. 6-13

Rid, T. (2012). *Cyber War Will Not Take Place*. The Journal of Strategic Studies. Vol. 35. No. 1. pp. 5-32

Robb, J. (2014, Enero 9). *Modern Militaries and a Network Centric Warfare Approach*. E-International Relations Students. http://www.e-ir.info/2014/01/09/modern-militaries-and-a-network-centric-warfare-approach

Slabodkin, G. (1998, Julio 13). *Software glitches leave Navy Smart Ship dead in the water*. https://gcn.com/Articles/1998/07/13/Software-glitches-leave-Navy-Smart-Ship-dead-in-the-water.aspx

Stone, J. (2015). *Coercion [Archivo PDF]*. Theory and Practice of War, King's College London

Stone, J. (2016, Enero 13). *US Confirms BlackEnergy Malware Used In Ukrainian Power Plant Hack*. http://www.ibtimes.com/us-confirms-blackenergy-malware-used-ukrainian-power-plant-hack-2263008

The Economist. (2013, Junio 29). *Digital doomsters.* https://www.economist.com/news/books-and-arts/21580123-how-scared-should-we-be-digital-doomsters

Zetter, K. (2015, Enero 8). *A Cyberattack Has Caused Confirmed Physical Damage For The Second Time Ever.* https://www.wired.com/2015/01/german-steel-mill-hack-destruction