

La Guerra en el Ámbito Cibernético

WELTON CHANG

SARAH GRANGER

DAR SENTIDO A LA ciberguerra requiere un entendimiento del ámbito cibernético. Las características intrínsecas del ámbito cibernético hacen que sea un reto determinar las implicaciones de la ciberguerra en la política de seguridad nacional. Es imprescindible definir correctamente el ámbito cibernético. Comprender cómo funciona y se comporta el medio ambiente al igual que las implicaciones de los conceptos, como por ejemplo la convergencia (la integración de tecnologías múltiples en un número más pequeño de plataformas y la armonización cada vez mayor del mundo virtual y del físico) ayudan a enmarcar el panorama más amplio.

El entorno cibernético le da forma a la porción “guerra” de la ciberguerra. Lamentablemente, las discusiones sobre la ciberguerra han sido polarizadas por los comentaristas, quienes algunos de ellos opinan que un “Pearl Harbo cibernético” es inevitable y otros opinan justamente lo contrario. La realidad radica en algún lugar en el medio. Resulta importante recordar que la guerra es una extensión de la política y que este axioma aplica en el ámbito cibernético. La planificación operacional debe tomar en cuenta el espectro de las amenazas. Comprender las implicaciones de la complejidad y las intenciones de los actores en el sistema será clave para crear estrategias eficaces de guerra cibernética.

Presentando el ámbito cibernético: Complejidad y transparencia

¿En qué consiste un ámbito cibernético?¹ La Internet, por supuesto, pero también mucho más. El ámbito cibernético incluye la arquitectura organizadora de la Internet, los dispositivos conectados a la Internet y las redes convencionales e inalámbricas. Algunas de esas redes son administradas por entidades del gobierno y del sector privado, algunas están conectadas a la Internet más amplia y algunas no. La escala de la Internet dificulta su comprensión. Esto nos conduce a un exceso de confianza en analogías imprecisas. Si bien técnicamente la Internet simple y llanamente es el primer ámbito creado por el hombre, su estructura puede ser difícil de conceptualizar. En lugar de existir dentro de fronteras finitas, imita otros sistemas naturales tales como colonias bacterianas y galaxias en expansión, donde billones de nódulos se expanden en todas las direcciones.² Como resultado, el ámbito cibernético, principalmente redes de computadoras conectadas, operando en un protocolo omnipresente de transferencia de datos, es complejo interactivo y estructuralmente.³

La complejidad hace que el ámbito cibernético sea difícil de estudiar. La complejidad estructural es el resultado del crecimiento exponencial del poder de la computación y la cantidad de dispositivos conectados a la Internet. La complejidad interactiva se deriva de la participación del ser humano en el sistema. El cambio tecnológico exponencial ha tornado el medio ambiente más complejo que nunca. Las cifras que ilustran este cambio son asombrosas: más de 2,1 mil millones de personas conectadas vía la Internet, 1,8 zettabytes de datos electrónicos creados en el 2011 y un total de 555 billones de sitios web. Se proyecta que en el 2016 la cifra de dispositivos móviles conectados a la Internet supere la cantidad total de personas en el planeta.⁴ La transacción de información entre cualquiera de esos dispositivos es posible, conduciendo a una multitud de interacciones y consecuencias que la humanidad aún tiene que comprender totalmente.⁵

La seguridad no formaba parte del diseño original del ciberespacio. El ámbito cibernético fue concebido para la transparencia. Los protocolos estandarizados para la transmisión de datos son el pegamento que mantiene junta a la Internet y los servicios para nombrar los ámbitos ayudan a dirigir los datos donde tienen que ir. Un diseño enfocado en la transparencia significa que la seguridad no es parte intrínseca en el sistema y debe ser injertada después. Cuando se crearon los protocolos no había mucho conocimiento del concepto de malware masivo a las computadoras. Las redes y el software creados encima de ellos viajan en una red central intrínsecamente abierta y, como resultado, hay que incorporar múltiples capas de seguridad para garantizar la integridad del sistema y los datos.⁶ Las vulnerabilidades esparcidas son semejantes a las deficiencias en el sistema inmunológico humano. La falta de variedad genética entre los seres humanos significa que enfermedades contagiosas pueden afectar a muchas personas. El ciberespacio tiene un tipo de uniformidad genética similar: la ubicuidad de los sistemas operativos como Microsoft Windows ejecutando programas como Internet Explorer significa que las vulnerabilidades no tratadas se esparcirán.

Describiendo el ámbito cibernético: Convergencia, el elemento humano, velocidad y asimetría

Más allá de la complejidad y la transparencia, varias características importantes del entorno cibernético le dan forma a la ciberguerra, inclusive niveles crecientes de convergencia, la velocidad de las interacciones, el elemento humano inextricable y facultar al individuo dentro del ámbito cibernético.

La convergencia es un concepto del cual se escribe a menudo, algunas veces se comprende y es criticado por muchos. La convergencia se ha referido en gran parte a la marcha aparentemente inexorable de la integración de tecnologías digitales en cada vez menos plataformas de entrega. Por ejemplo, la diferencia entre el correo electrónico, la televisión y las comunicaciones por voz ha sido nublada por la adopción a gran escala de smartphones capaces de llevar a cabo las tres funciones operando en protocolos de Internet. La convergencia también es la unión de los mundos virtual y físico. A medida que más sistemas estén conectados a una Internet más amplia para fines de eficacia y conveniencia, muchos objetos físicos tendrán una presencia en el mundo virtual. En un extremo, la eliminación virtual se convierte en el equivalente de la destrucción física. Por ejemplo, la mayoría de las finanzas del mundo existen solamente como datos, y arreglar la corrupción de datos dependería de datos electrónicos a falta de expedientes físicos.⁷ La unión de los mundos físico y virtual también se ha extendido a los humanos y la tecnología. La convergencia también significa que las vulnerabilidades identificadas actualmente en programas de computadora que controlan entidades físicas tales como los sistemas de control industrial (ICS, por sus siglas en inglés) se esparcirán aún más.⁸ ICS es el término genérico para una clase de sistemas electrónicos que controlan una gama amplia de infraestructura tales como los sistemas de agua, gas y eléctricos. En un sistema intrínsecamente abierto, la convergencia significa más vulnerabilidades virtuales, algunas análogas a las físicas.

El elemento humano es una parte fundamental del ámbito cibernético que no se puede pasar por alto. En vista de que seres humanos construyeron la arquitectura cibernética, será intrínsecamente imperfecta. Además, hacer cumplir las medidas de seguridad tales como la instalación de software antivirus, la creación de contraseñas difíciles y el rechazo de tácticas de ingeniería social tales como "phishing", recae sobre el usuario. Y en la mayoría de los casos, el software en sí tiene fallas, ya sea si se encuentra en el sistema operativo o al nivel de aplicación.

La velocidad también es un elemento importante del ámbito cibernético que se debe tomar en cuenta cuando se opera en el ciberespacio. La acción en el ciberespacio puede ser más rápida y puede conducir a efectos geográficos de mayor alcance que en otros ámbitos. Sin embargo, los

operadores de los sistemas de computadoras son seres humanos que no trabajan a la velocidad de la luz. Los humanos actúan como restricciones funcionales en el medio ambiente hasta el punto que están en control del dispositivo y un programa en funcionamiento. Sin bien los electrones se mueven a la velocidad de la luz, embotellamientos en la arquitectura de la red y la velocidad del procesador común a lo largo de una ruta de datos también son restricciones. Por último, si bien los electrones son más rápidos que las fuerzas terrestres, cuando las operaciones en el ciberespacio apoyan operaciones militares de mayor escala en otros ámbitos, las fuerzas refrenan el ritmo de las operaciones. En un final, el esfuerzo principal también dicta la eficacia de los electrones.

El ámbito cibernético es un entorno operacional en el que la eficacia del individuo es ampliada a causa de la automatización, la agilidad de grupos pequeños y la difusión del conocimiento a lo largo de las geografías. Un individuo operando en cualquier parte del mundo con una conexión a la Internet puede estar al mando de un botnet (un grupo de computadoras controladas clandestina y remotamente) grande y a menudo involuntario para llevar a cabo ataques de negación de servicio. Un individuo también puede crear un programa que se reproduce y extiende por sí solo, a través de la misma vulnerabilidad. En vista de que la transmisión de conocimiento ahora es prácticamente gratuita, los individuos en redes de cooperación pueden aprender rápidamente las técnicas de ataque más eficaces y aprovecharse de vulnerabilidades anteriormente desconocidas. Esas redes de cooperación y redes de redes comienzan a dar muestras de inteligencia emergente, reproduciendo acciones dirigidas centralmente cuando no existe ese tipo de autoridad. Esto significa que individuos tales como el grupo Anonymous, empleando un botnet, puede tener el mismo impacto que los operativos de computadora que desactivaron grandes cantidades de redes estonianas públicas y privadas en el 2007.⁹

Por último, la asimetría entre los recursos, costos, valores, intereses y organización de grupos tales como Anonymous en comparación con organizaciones gubernamentales tales como el Comando Cibernético de Estados Unidos estriba de un medio ambiente que está más dispuesto a la insurgencia virtual que a la guerra convencional.¹⁰ En vista del diseño abierto del ámbito ciberespacial, la defensa es intrínsecamente más costosa y toma más tiempo que la ofensiva. Además, armas cibernéticas costosas y sumamente técnicas creadas por gobiernos se pueden rediseñar fácil y económicamente por otros en el ámbito ciberespacial. La asimetría en el ámbito ciberespacial por lo general favorece a actores más pequeños y más ágiles. A menudo esos actores no cuentan con una dirección física permanente y pueden enmascarar sus direcciones virtuales. Este es un punto clave que las burocracias grandes tienen que adoptar para poder crear estrategias eficaces de mitigación.

Clausewitz Cibernético

La primacía de la política en la ejecución de cualquier tipo de guerra significa que en un final la guerra es una contienda de voluntad política. Cuando las estrategias se crean correctamente, los objetivos políticos serán la meta final de la ciberguerra. Algunos comentarios sobre la ciberguerra se enfocan en las características singulares del ámbito cibernético, a la vez que pasan por alto la idea de que la guerra es una extensión de la política. En los argumentos de si un "Pearl Harbor cibernético" es o no inevitable, los comentaristas rara vez toman en cuenta la idea que dicha acción extrema sería emprendida para fines políticos.¹¹ De manera similar, cuando se discute el ciberterrorismo, un "11-S cibernético" se describe como imposible o inevitable.¹²

Un "Pearl Harbor cibernético" probablemente no ocurrirá a menos que los beneficios de tomar dicha acción superan los costos para un estado. Por ejemplo, la integración de las economías estatales aumentan los costos de la acción unilateral. Algunos parecen pensar que el plural de los ataques cibernéticos es la guerra cibernética pero no debemos olvidar que la guerra exige

un objetivo político. Inclusive los actos terroristas están concebidos para lograr algún tipo de objetivo político o religioso, ya sea desmoralizar una población u obligar a un gobierno a negociar, no solamente destruir por destruir. Entender las intenciones de los adversarios es primordial al igual que lo es reconocer hasta el punto al cual un adversario dependería de otros actores en el sistema. En el mundo hiperintegrado en el que vivimos, no tomar en cuenta la dependencia nos conduce a obviar el factor clave en la probabilidad o poca probabilidad de que estalle una guerra. Por último, la ciberguerra no tiene que ocurrir en las partes extremas del espectro de la capacidad. Enfocarse en la discusión de escenarios extremos solo sirve para polarizar argumentos y ofuscar los peligros verdaderos que existen.

La situación real actual

¿Ya hemos presenciado la ciberguerra?¹³ Las acciones rusas pretendidas durante el conflicto con Estonia en el 2007 son el primer ejemplo y a menudo el más mencionado. Algunos expertos creen que el uso de las tácticas cibernéticas durante la disputa con Estonia en el 2007 fue más semejante a un conflicto cibernético, que no está a la altura del umbral de la guerra.¹⁴ Sin embargo, en el 2007 ni los estados ni las poblaciones dependían tanto del ámbito cibernético como dependen ahora. La informática de nube apenas estaba comenzando y su dependencia en la Internet para el comercio y la banca era infinitamente diferente.

Las vulnerabilidades intrínsecas en el ámbito cibernético, junto con el desarrollo de las capacidades de varios actores (algunos con intenciones malignas) significa que la ciberguerra es una posibilidad muy real en el futuro. Cualquier estrategia nacional cibernética que busque lidiar con el medio ambiente cibernético debe tomar en cuenta los riesgos si no se tratan las vulnerabilidades. Con base en nuestro nivel de dependencia en el ámbito cibernético tanto para las capacidades de seguridad nacional como el funcionamiento de la vida cotidiana, los riesgos son grandes.¹⁵

Pero, ¿cuál es el nivel actual de la amenaza? Esto es difícil de definir por varias razones, aunque podemos decir con certeza que durante los dos últimos años, los ataques a redes y sistemas principales han crecido consistentemente, tanto en situaciones públicas como en el sector privado.¹⁶ Resulta difícil recopilar y analizar estadísticas exactas con respecto a los ataques, y un enfoque en las estadísticas del ataque pasa por alto la amenaza más insidiosa de ataques no detectados y vulnerabilidades no explotadas en el software y hardware.¹⁷ Organizaciones y sectores diferentes pueden albergar intereses provincianos con respecto a exagerar o disminuir el panorama de la amenaza.¹⁸ Ya sea que esos intereses sean burocráticos o impulsados por las ganancias, los análisis de la amenaza deben juntarse y destilarse para lograr un entendimiento más holístico e imparciales de la situación real actual. También es posible que ataques a gran escala se vean muy diferentes de lo que se ha experimentado anteriormente.¹⁹

Cuando se trata de ciberguerras hay un espectro de amenazas y tácticas, desde negación de servicio a interrupción hasta la destrucción de hardware físico conectado vía los sistemas de control industrial. Este espectro de amenazas llega a todos los demás ámbitos de la guerra—terrestre, marítima, aérea y espacial.²⁰ La dimensión económica también es tremenda—el General Keith Alexander, jefe del Comando Cibernético de EE.UU. y de la Agencia de Seguridad Nacional de EE.UU., expresó que las amenazas y los ataques cibernéticos existentes constituyen la mayor “transferencia de riqueza en la historia”.²¹ Para una institución de defensa estadounidense que depende tanto de una ventaja económica y material abrumadora, esto equivale a una “muerte segura”.²²

Una conclusión razonable es que podría sufrir una amplia gama de ataques posibles, especialmente en un conflicto mundial real que tiene lugar a lo largo de otros ámbitos.²³ Es probable que el ciberterrorismo se convierta más en un conocimiento acerca de propagaciones de siste-

mas de control industrial mientras que las vulnerabilidades seguirán sin tratarse. Por último, ha habido cierto movimiento hacia los ataques cibernéticos de precisión, programas complejos de computadoras que funcionan para lo que fueron concebidos podría resultar en consecuencias catastróficas no intencionales a falta de la interacción humana.²⁴

En conclusión: Educar, entrenar y coordinar

Si se permite que nuestras vulnerabilidades cibernéticas continúen sin tratarse, estamos dejando bajar el puente levadizo virtual.²⁵ Nuestra labor ahora es mejorar el intercambio de información, los esfuerzos de inteligencia y los mecanismos para coordinar la seguridad de manera que podamos evitar, adaptarnos y reaccionar en caso de que llegue el momento en que se comprometan la infraestructura crítica u otras redes importantes. Debemos actuar ahora porque la infraestructura crítica le da poder a nuestra economía y a nuestro aparato de seguridad nacional.

Avanzando, continuar educando a todos los interesados civiles y militares es de suma importancia, además de asegurar las redes y nodulos en sí. Un problema que se avecina es que la cantidad de norteamericanos que se están entrenando, educando y desarrollándose dentro de Estados Unidos (inclusive estudiantes universitarios especializándose en ciencias computacionales y campos afines) no está aumentado correctamente para igualar la amenaza creciente. También es importante educar a los ciudadanos en general acerca de mejorar la seguridad en sus computadoras y redes. Un método híbrido para administrar la amenaza cibernética, la respuesta en casos de incidentes y las medidas defensivas preplanificadas se debe adoptar para poder crear una arquitectura defensiva más resistente.²⁶

En el futuro cercano veremos más software para recopilar inteligencia en nuestras redes, experimentaremos más ataques generalizados de distintos tipos y debemos esperar enfrentarnos a consecuencias imprevistas e interrupciones que aún no se han visto. Si bien en la mayoría de los casos la naturaleza de los ataques puede que sea impredecible, la historia será una guía confiable para otros. Lo que sí sabemos es que distintos tipos de adversarios—individuos, grupos parias y organizaciones sofisticadas—ya radican en redes y pueden penetrarlas a su antojo en muchos casos.

Hasta cierto punto hemos sido afortunados. En algunas ocasiones los ataques en la infraestructura crítica y otros sistemas importantes han sido frustrados y esa información se ha compartido con el público.²⁷ Esos episodios disipan el mito que no hay motivo para que los agresores ataquen esos sistemas. La resistencia de los modelos es eficaz en planificar la recuperación y respuesta, particularmente a causa de la naturaleza asimétrica del ámbito y la probabilidad de patrones de ataque complejos y de muchas fases. Una educación exitosa en este campo debe incluir entrenamiento en resistencia, prácticas de respuesta en un escenario al igual que ingeniería técnica y social. El diseño de módulos de entrenamiento que se puedan desplegar rápidamente podría ser sumamente útil. En muchos casos, el proceso de obtener permiso para ofrecer programas de educación y entrenamiento puede ser un obstáculo por derecho propio, evitando que personal a todos los niveles obtengan destrezas muy necesarias que pueden ser útiles para identificar y combatir ataques cibernéticos.

En un final, la complejidad y las propiedades intrínsecas del entorno cibernético no nos deben detener de trazar estrategias y planificar.²⁸ Mientras que la inmensidad del ámbito cibernético abruma nuestra infraestructura vertical no integrada gubernamental, nuestro entendimiento colectivo mejora cada año aunque la amenaza continúa creciendo. Pero al incorporar la resistencia al sistema y distribuir la responsabilidad defensiva a todos los usuarios finales, llevar a cabo una guerra en el ámbito cibernético se tornará más costosa y menos eficaz para el agresor. Puede que la ciberguerra aún no haya ocurrido, pero es verdaderamente una amenaza futura que los gobiernos, empresas privadas e individuos deben tomar en serio. La amenaza está au-

mentando y al tomar medidas ahora para aumentar la seguridad, disminuimos el riesgo de ser sorprendidos desprevenidamente. □

Notas

1. En la Joint Publication (Publicación Conjunta) 1-02 se define el ciberespacio como “un ámbito global en el entorno de información que consta de la red independiente de infraestructuras de tecnología de la información, inclusive la Internet, redes de telecomunicaciones, sistemas de computadoras y procesadores y controladores incorporados”. United States Department of Defense, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (Diccionario de Términos Militares y Afines del Departamento de Defensa), (Washington D.C.: 8 de noviembre de 2010), págs. 79-80; consultado en: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

2. Por publicarse: Sarah Granger, Lorelei Kelly, “Cybersecurity and Modern Grand Strategy” (Ciberseguridad y la gran estrategia moderna), Institute for the Study of Diplomacy, Georgetown University School of Foreign Service, 2012; pág. 1.

3. Ver: United States Army Training and Doctrine Command, “TRADOC Pamphlet 525-5-500: Commander’s Appreciation and Campaign Design” (Folleto TRADOC 525-5-500: Evaluación del Comandante y diseño de la campaña), 28 de enero de 2008, págs. 5-7; consultado en: <<http://www.tradoc.army.mil/tpubs/pams/p525-5-500.pdf>>.

4. Ver: Pingdom, “Internet in 2011 in numbers” (La Internet en cifras en el 2011), Royal Pingdom, 17 de enero de 2012; consultado en: <<http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/>>. Jon Brodtkin, “Mobile internet devices will outnumber humans this year, Cisco predicts” (Cisco predice que los dispositivos móviles de Internet sobrepasarán la cifra de seres humanos este año), Ars Technica, 14 de febrero de 2012; consultado en: <<http://arstechnica.com/business/2012/02/mobile-internet-devices-will-outnumber-humans-this-year-cisco-predicts/>>; IDC, “The 2011 Digital Universe Study: Extracting Value From Chaos” (Estudio del universo digital 2011: Extrayendo valor del caos), junio de 2011; consultado en: <<http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm>>.

5. En un estudio JASON de MITRE sobre la seguridad cibernética se alega que, “No hay “leyes de naturaleza” intrínsecas para la seguridad como las hay, por ejemplo, en física, química o biología. La ciberseguridad es esencialmente una ciencia aplicada que es informada por los conceptos matemáticos de la ciencia computacional tales como teoría automática, complejidad y lógica matemática”. JASON, “Science of Cyber Security” (La ciencia de la ciberseguridad), MITRE Corporation, noviembre de 2010, pág. 4; consultada en: <<http://www.fas.org/irp/agency/dod/jason/cyber.pdf>>.

6. Ver: Paul A. Strassaman, “The Internet’s Vulnerabilities Are Built Into Its Infrastructure” (Las vulnerabilidades de la Internet están incorporadas a su infraestructura), AFCEA, Signal Online, noviembre de 2009; <http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2109&zzoneid=3>.

7. Para un ejemplo de los peligros de la convergencia ver: Robert O’Harrow Jr., “Tridium’s Niagara Framework: Marvel of Connectivity Illustrates New Cyber Risks, (Estructura Niágara de Tridium: Maravilla de conectividad ilustra nuevos riesgos cibernéticos)” Washington Post, 11 de julio de 2012, consultado en: <http://www.washingtonpost.com/investigations/tridium-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html>.

8. Ver: Keith Stouffer, Joe Falco, and Karen Scarfone, “Guide to Industrial Control Systems” (Guía para los sistemas de control industriales), National Institute of Standards and Technology”, NIST Special Publication 800-82, pág. 2-1; consultado en: <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800.82.pdf>>. Supervisory Control and Data Acquisition Systems (SCADA) (Los sistemas de supervisión de control y adquisición de datos [SCADA]) son una clase de sistemas de control industrial. Programas como SCADAscan detectan redes SCADA conectadas a la Internet. Ver también: Bill Brenner, “#BSidesSF: Why SCADA security is such an uphill struggle” (#BSidesSF: Por qué la seguridad SCADA es una ardua batalla), CSO Online, 27 de febrero de 2012; consultado en: <<http://blogs.csoonline.com/critical-infrastructure/2044/bsidessf-why-scada-security-such-uphill-struggle>>.

9. Se sospecha que piratas cibernéticos rusos o pro rusos han perpetrado ataques de negación de servicio contra sitios del gobierno estoniano y del sector privado durante un conflicto sobre la reubicación de un monumento de guerra. Ver: William C. Ashmore, “Impact of Alleged Russian Cyber Attacks” (Impacto de presuntos ciberataques rusos), US Army School of Advanced Military Studies, mayo de 2009, págs. 5-8; consultado en: <<http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA504991>>.

10. Para una discusión sobre asimetría y la ciberguerra ver: Michael Breen, Joshua A. Geltzer, “Asymmetric Strategies as Strategies of the Strong” (Estrategias asimétricas como estrategias del fuerte), Parameters, primavera 2011, págs. 48-49; consultado en: <<http://www.carlisle.army.mil/usawc/parameters/Articles/2011spring/Breen-Geltzer.pdf>>. También ver: Quinn Norton, “How Anonymous Picks Targets, Launches Attacks, and Takes Down Powerful Organizations” (Cómo anónimos seleccionan blancos, lanzan ataques y destruyen organizaciones poderosas), Wired, 3 de julio de 2012, consultado en: <http://www.wired.com/threatlevel/2012/07/ff_anonymous/all/>.

11. Un “Pearl Harbor cibernético” en nuestro cálculo sería un ataque debilitante masivo, intencional e inesperado a la infraestructura crítica y capacidades de defensa de EE.UU. Ver: Jake Tapper, “Leon Panetta: A Crippling Cyber Attack Would Be An Act of War” (Leon Panetta: Un ciberataque de consecuencias catastróficas sería un acto de guerra), ABC News, 27 de mayo de 2012; consultado en: <<http://abcnews.go.com/blogs/politics/2012/05/leon-panetta-a-crippling-cyber-attack-would-be-act-of-war/>>.

12. Sunlen Miller, “Despite Threat of ‘Cyber 9/11’, Lawmakers Punt Cyber Security Bill” (A pesar de la amenaza de un 11-S cibernético, los encargados de formular leyes desaprueban proyecto de ley sobre ciberseguridad), ABC News, 2 de agosto

de 2012; consultado en: <<http://abcnews.go.com/blogs/politics/2012/08/despite-threat-of-cyber-911-lawmakers-punt-cyber-security-bill>>.

13. Este es un debate que ha ocurrido varias veces durante los últimos diez años. Ver: Intelligence Squared, "The Cyber War Threat Has Been Greatly Exaggerated" (La amenaza de la ciberguerra se ha exagerado demasiado), 8 de junio de 2010; consultado en: <<http://intelligencesquaredus.org/debates/past-debates/item/576-the-cyber-war-threat-has-been-grossly-exaggerated>>. Ver también: David Betz, "Cyberwar' is not coming" (La ciberguerra no ocurrirá), Infinity Journal, Volume 1 Issue 3.

14. Contraalmirante (ret.) Michael McConnell, "Cyber-Power and Cyber-Security" (Poder cibernético y seguridad cibernética), Aspen Security Forum, 1 de julio de 2012; consultado en: <<http://www.aspenideas.org/session/cyber-power-and-cyber-security>>. Thomas Rid alega que el umbral que la ciberguerra debe cumplir es que "tiene que ser potencialmente violento, con una finalidad y tiene que ser político". Aquellos que alegan que la ciberguerra no ha ocurrido creen que la falta de violencia y la destrucción física hacen que la acción cibernética no sea del orden de una guerra cibernética. Thomas Rid, "Think Again: Cyberwar" (Piensen nuevamente: Ciberguerra), Foreign Policy, marzo/abril de 2012, consultado en: <<http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full>>.

15. Un aspecto crítico del cual civiles y militares dependen es el sector de generación de potencia. Ver: Reuters, "Senators to hear pitch for tougher cyber security" (Los senadores escucharán oferta para seguridad cibernética más fuerte), 12 de marzo de 2012, consultado en: <<http://www.reuters.com/article/2012/03/07/us-usa-cybersecurity-congress-idUSTRE82621W20120307>>.

16. David Sanger, Eric Schmitt, "Rise is Seen in Cyber Attacks Targeting U.S. Infrastructure" (Se ve aumento en ciberataques que se concentran en la infraestructura de EE.UU.), The New York Times, 26 de julio de 2012, consultado en: <<http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html>>. Ver también: James A. Lewis, "Significant Cyber Events" (Eventos cibernéticos significativos), Center for Strategic and International Studies, última actualización mayo de 2012; consultado en: <<http://csis.org/publication/cyber-events-2006>>.

17. Conocidas anteriormente pero existentes, las vulnerabilidades incluyen vulnerabilidades de hardware y de software conocidas como explotaciones de "día cero". La dificultad en atribuir el ataque (saber quién lo hizo) es también una preocupación importante en el ámbito cibernético. Ver también: Sergei Skorobogatov, Christopher Woods, "In the blink of an eye: There goes your AES key" (En un abrir y cerrar de ojos: Ahí va su clave AES), 28 de mayo de 2012, consultado en: <<http://eprint.iacr.org/2012/296.pdf>>.

18. Para una discusión sobre este tema, ver: consultado en: Peter Maass, Megha Rajagopalan, "Does Cybercrime Really Cost \$1 Trillion?" (¿En realidad el crimen cibernético cuesta \$1 trillón de dólares), Propublica, 1 de agosto de 2012; <<http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion>>.

19. Frank Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Conflicto en el siglo XXI: El surgimiento de las guerras híbridas), consultado en: <http://www.potomac institute.org/index.php?option=com_content&view=article&id=77:-conflict-in-the-21st-century-the-rise-of-hybrid-wars&catid=40:books&Itemid=62>.

20. Danny Steed, "Cyber Power and Strategy: So What?" (Poder y estrategia cibernética: ¿Y qué?), Infinity Journal, Vol. 1 Issue 2, consultado en: <http://www.infinityjournal.com/article/11/Cyber_Power_and_Strategy__So_What?>.

21. Michael Riley y Dune Lawrence, "Hackers Linked to China's Army Seen from E.U. to D.C." (Piratas cibernéticos conectados con el Ejército Chino vistos desde la UE hasta DC), Bloomberg, 26 de julio de 26, 2012; consultado en: <<http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html>>.

22. Cheryl Pellerin, "Cyber Operations Give Leaders New Options, Official Says" (Según funcionarios, las operaciones cibernéticas les ofrecen nuevas opciones a los líderes), American Forces Press Service, 12 de abril de 2012; consultado en: <<http://www.defense.gov/news/newsarticle.aspx?id=67918>>. Tanto James Lewis de CSIS y Richard Clarke también han empleado esta analogía.

23. Para una discusión de la presunta carrera armamentista cibernética, ver: Michael Riley, Ashlee Vance, Cyber Weapons: The New Arms Race (Armamento cibernético: La nueva carrera armamentista), Bloomberg Businessweek, 20 de julio de 2011, consultado en: <<http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p1>>.

24. Por ejemplo, ver el impacto del comercio automatizado de alta velocidad en Wall Street. Nathaniel Popper, "Knight Capital Says Trading Glitch Cost it \$440 Million", (Knight Capital alega que el percance del comercio le costó \$440 millones de dólares), The New York Times, 2 de agosto de 2012, consultado en: <<http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/>>.

25. Stewart Baker, Natalia Filipiak, Katrina Timlin, "In the dark: Crucial industries confront cyberattacks" (En la oscuridad: Industrias cruciales enfrentan ciberataques), McAfee, Center for Strategic and International Studies, 2011; consultado en: <<http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf>>.

26. El estratega norteamericano T. X. Hammes declara que lidiar con "grupos pequeños sumamente fortalecidos" requiere una "respuesta de toda la sociedad" y que ese modelo está presente en "la defensa de la Internet". Ver: Jim Zirin, "Will the war in the 21st Century be fought in cyber space?" (¿Se librará la guerra del siglo XXI en el ciberespacio?), Digital Age, 25 de noviembre de 2007, 20:26-20:28; consultado en: <http://www.youtube.com/watch?v=j1_QG0NlwdE>. Charles Billo, Welton Chang, Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States, (Ciberguerra: Un análisis de los medios y motivaciones de naciones estados exclusivas), Institute for Security Technology Studies, (Hano-

ver, NH: Dartmouth College, diciembre de 2004), pág. 133; consultado en: <<http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>>.

27. Mark Clayton, "Report: Cyberattacks on critical US targets surge" (Informe: Aumentan ciberataques en blancos críticos estadounidenses), Christian Science Monitor, 29 de junio de 2012, consultado en: <<http://www.csmonitor.com/USA/2012/0629/Report-Cyberattacks-on-critical-US-targets-surge>>. La operación Dragón Nocturno fue un grupo de ataques publicados contra compañías de energía. La operación Shady Rat atacó, según informes, 70 víctimas gubernamentales, del sector privado y sin fines de lucro en 40 países. Ver: Dmitri Alperovitch, "Revealed: Operation Shady RAT" (Revelada: Operación Shady RAT), McAfee, versión 1.1, 2012, consultado en: <<http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>> y McAfee, "Global Energy Cyberattacks: Night Dragon" (Ciberataques a la energía global: Dragón Nocturno), 10 de febrero de 2011, consultado en: <<http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>>.

28. Michael J. Gallagher, Joshua A. Geltzer, y Sebastian L.V. Gorka, "The Complexity Trap" (La trampa de la complejidad), Parameters, primavera de 2012, consultado en: <http://www.carlisle.army.mil/usawc/Parameters/Articles/2012spring/Gallagher_Geltzer_Gorka.pdf>. También ver: Sarah Granger, Lorelei Kelly, "Cybersecurity and Modern Grand Strategy", Institute for the Study of Diplomacy, Georgetown University School of Foreign Service, 2012.



El Sr. Welton Chang es un analista en el Departamento de Defensa. Fue el asesor principal civil en el 2011 en la Célula de Inteligencia Nacional de Iraq. Desde el 2005 al 2012 Welton se desempeñó como oficial del servicio activo y de la reserva del Ejército. Durante ese tiempo fue desplegado a Iraq y Corea del Sur. En el 2005, Welton egresó cum laude del Dartmouth College con altos honores de la facultad. Mientras asistió a Dartmouth, Welton trabajó en el Institute for Security Technology Studies (Instituto de Estudios de Tecnología de Seguridad) donde fue coautor y publicó una monografía muy mencionada sobre la guerra cibernética. En la actualidad es candidato para una Maestría en el Programa de Estudios de Seguridad de la Georgetown University. Además es un becado de Truman National Security Project (Proyecto Truman de Seguridad Nacional).



La Srta. Sarah Granger es la fundadora del Center for Technology, Media & Society (CFTMS) (Centro de Tecnología, Medios de Comunicación y Sociedad). Actualmente es becada del Truman National Security Project, donde es co-presidenta de su grupo de ciberseguridad. Comenzó su carrera trabajando en ciberseguridad para el Lawrence Livermore National Laboratory, seguido por trabajo como asesora de seguridad en la red varios años antes de fundar CFTMS. Sarah fue autora colaboradora de Ethical Hacking, y ha editado varios libros sobre seguridad móvil, criptografía y biométrica. Además, ha escrito para Spectrum, Security Focus, y Forbes Russia. Pueden seguirla en Twitter @sarahgranger.

Las opiniones expresadas en este artículo son las de los autores y no reflejan ni la política oficial ni la postura de la Agencia de Inteligencia de la Defensa, ni del Departamento de Defensa, ni de ninguna agencia del gobierno de Estados Unidos.