(Foto: Fuerza Aérea de EUA)

La seguridad cibernética

Ya no solo es para los oficiales de transmisión

Teniente Coronel (retirado) D. Bruce Roeder, Ejército de EUA

El teniente coronel (retirado) D. Bruce Roeder, Ejército de EUA, es instructor en el Departamento de Educación a Distancia en la Escuela de Comando y Estado Mayor General del Ejército de EUA, en el Fuerte Leavenworth, estado de Kansas. Es egresado de la Academia Militar de Estados Unidos y cuenta a su haber con una Maestría de la Universidad Webster. El teniente Col Roeder sirvió previamente en una variedad de posiciones en calidad de oficial preboste, oficial de seguridad y oficial de operaciones.

"¡SIGO!, fue el grito que se escuchó en el comedor cuando el micrófono de megafonía del estrado en el salón del club de oficiales no funcionó. Los carnívoros en la unidad se sonreían de oreja a oreja de puro alivio mientras que el pobre SIGO (oficial de transmisión) valientemente luchaba para arreglar el malfuncionamiento del podio para que trabajara como debía. Así es como algunos de nosotros hemos abordado el tema de la seguridad cibernética: es la jurisdicción del tipo lleno de alambres en la cabeza, y ¡gracias a Dios!

Bien, si alguna vez fue así, ya no lo es más. Cuando el director de Inteligencia Nacional, James R. Clapper, emitió la Evaluación de Amenaza Mundial de 2013 de la Comunidad de Inteligencia para el Comité del Senado sobre Inteligencia, las amenazas cibernéticas en su lista de amenazas globales a la seguridad nacional de Estados Unidos aparecieron por delante del terrorismo y de las armas de destrucción masiva.[1] De hecho, los ataques cibernéticos constantemente están en las noticias. El experto en seguridad cibernética y oficial de la reserva, H. Mikko Hypponen, postula que en los países desarrollados, la gente está más propensa a ser víctima de la delincuencia en Internet que del crimen "en la vida real". Con la naturaleza ubicua de las interacciones en línea de la vida moderna, las amenazas cibernéticas constituyen una amenaza de seguridad principal para los individuos y la Nación. Entonces, ¿qué es lo que hace ese frenético SIGO, poniendo todo su empeño para que esa cosa funcione correctamente?

Echemos un vistazo a la difícil situación que enfrenta nuestro SIGO. En primer lugar, en términos sencillos, hay tres clases típicas de ataques cibernéticos que presentan una amenaza: delictivos, ideológicos y Estado-nación. Por lo regular, los criminales profesionales están motivados por la codicia. Caen bajo la jurisdicción de la ley, aunque la tecnología que usan tiende a ir más allá de las capacidades de las agencias de policía ordinaria. Luego, le sigue la ideología y los llamados "piratas activistas", como *WikiLeaks* o *Anonymous* que, por lo general, son motivados por su visión política o filosófica del mundo, o tal vez por el cinismo. A menudo, anuncian sus blancos y, a veces, efectúan ataques solo para llamar la atención o burlarse. La ley también los trata como criminales. El tercer tipo es Estados-nación, que generalmente son motivados por seguridad, economía u otros intereses. Pueden planear y ejecutar ataques cibernéticos coordinados contra sus enemigos. Normalmente, tienen acceso a más recursos que los criminales y los ideólogos. No siempre es fácil asignar una categoría especial a los ataques cibernéticos. Además, para enturbiar más las aguas, queda la incógnita de si un ataque cibernético se considera como uso de la fuerza.

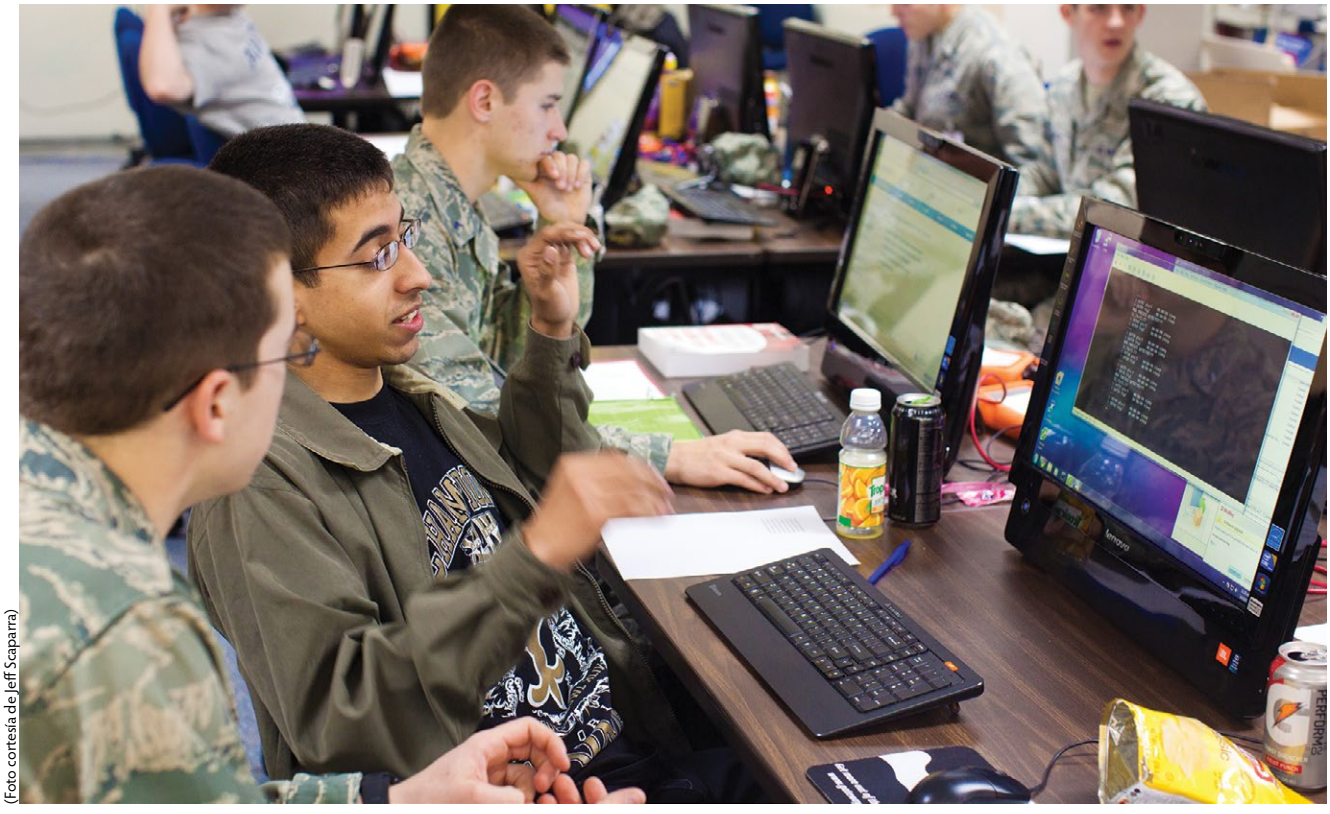
Por otra parte, resulta difícil determinar cuáles amenazas cibernéticas específicas son más peligrosas para la seguridad nacional de Estados Unidos y cuál es más probable que ocasione daños. Las amenazas cibernéticas surgen de manera inesperada. Por ejemplo, *Stuxnet*, el malware diabólicamente destructivo que buscó las centrifugadoras en la instalación de enriquecimiento de uranio en Natanz, Irán, ahora representa una amenaza mucho mayor que la de su propósito original. Esto es porque el código usado para construir *Stuxnet* (descubierto en 2010 y ampliamente considerado como un ataque cibernético patrocinado por el Estado) se filtró inadvertidamente en Internet. Algunos analistas creen que sus descendientes (como *Duqu* y *Flame*) o su progenie, ya podrían estar residiendo en las bases de datos de infraestructuras criticas a nivel mundial.[3] Las cosas malas que están ocurriendo van más allá de cualquier conjunto de destrezas o recursos de SIGO. ¿Cómo deberíamos responder en este momento?

¿Más burocracia?

La respuesta típica y hasta obligatoria del gobierno es darle a una oficina o agencia la responsabilidad y los recursos para solucionar un problema. Este planteamiento previsible, lento y de arriba abajo para resolver problemas a nivel nacional es ineficaz contra un problema incierto, cambiante y de abajo arriba. Por ejemplo,

el Departamento de Defensa estableció el Comando Cibernético de Estados Unidos (USCYBERCOM, por sus siglas en inglés), un comando sub-unificado subordinado al comando estratégico de Estados Unidos. Los componentes de servicio debidamente se organizan para prestar apoyo. El Ejército cuenta con el Comando Cibernético del Ejército de Estados Unidos, la Marina cuenta con el Comando Cibernético de Flota de EUA, la Fuerza Aérea cuenta con la 24ª Fuerza Aérea (Fuerzas Aéreas Cibernéticas) y el Cuerpo de la Infantería de Marina cuenta con el Comando Cibernético de las Fuerzas de la Marina. Sin embargo, independientemente de cuán capaces sean estas unidades, principalmente se centran en las amenazas contra la seguridad cibernética de las redes de información de defensa de Estados Unidos. Por otro lado, "a menudo, el gobierno no está consciente de la actividad maliciosa dirigida hacia nuestra infraestructura crítica", expresó el general Keith Alexander, ex jefe de la Agencia Nacional de Seguridad y USCYBERCOM.[4]

Cuando se trata del sector civil, el congresista estadounidense, Mike Rogers, del Estado de Michigan, dice que "hoy estamos en una sigilosa guerra cibernética... y estamos perdiendo.[5] Sin embargo, no cabe duda de que los líderes empresariales estadounidenses se dan cuenta de que la amenaza cibernética es verdadera y tendrán que trabajar estrechamente con el gobierno para prevenir un gran ataque o estar preparados para responder con eficacia a uno. Para ellos, si algo afecta sus ganancias, es importante. Aún así, en la actualidad, las empresas tienen poco incentivo para alertar a los funcionarios federales después de haber sido atacados cibernéticamente porque los federales luego comparten esa información con sus competidores. Por otra parte, si los negocios comparten cierta información con algunos de sus competidores, corren el riesgo de persecución por parte del gobierno bajo las leyes antimonopolio. Por lo tanto, a menos que las corporaciones tengan cierta protección de responsabilidad o de perder su ventaja competitiva, es improbable que colaboren voluntariamente. Las protecciones legales deben ser codificadas por el Congreso, pero el Congreso no ha aprobado ninguna legislación sobre la seguridad cibernética desde 2002. El 12 de febrero de 2013, el presidente Obama emitió una orden ejecutiva llamada "Cómo mejorar la seguridad cibernética de la infraestructura crítica"



(Foto cortesía de Jeff Scaparra)

Cadete 4ª Clase Anthony Canino, izquierda, y Cadete 2ª Clase Matthew Toussain, hablan sobre las defensas de la red durante una clase de National Collegiate Cyber Defense competencia regional "At Large" en la Academia de la Fuerza Aérea, 6 de marzo de 2011.

como una medida provisional para proteger a los negocios del litigio antimonopolio, si voluntariamente comparten datos con sus competitores.[6] Aún cuando el Congreso actúe, la participación seguramente seguirá siendo voluntaria por parte de la infraestructura económica de propiedad privada.

El cuidado y la alimentación del aparato de seguridad cibernética del gobierno (incluyendo contratistas afiliados) seguramente nos permitirá obtener y mantener contacto con las amenazas cibernéticas, pero es poco probable que ese aparato pueda tomar la iniciativa del enemigo. Pareciera que nos enfrentamos al problema como un toro en una tienda de porcelana. Se necesita algo más para resolver el problema.

La característica definitoria de la *World Wide Web* es que está por todo el mundo; la fuerza misma de Internet es su carácter internacional. Esa es precisamente la característica que permite a los piratas, los delincuentes cibernéticos y su dinero, revolotear rápida y fácilmente de un país a otro hasta tanto se identifican cuidadosamente y se cierran sus sitios web. Es muy importante para una iniciativa eficaz de seguridad cibernética contar con la misma capacidad para cruzar las jurisdicciones internacionales. Las agencias deben poder coordinar con organismos similares en todo el mundo tan ágilmente como lo hacen los criminales. La página web del Instituto para el Crimen Interregional e Investigación de Justicia de las Naciones Unidas (UNICRI, por sus siglas en inglés) ofrece perspectivas sobre cómo este planteamiento operacional podría funcionar.[7] Si bien el UNICRI es una agencia pequeña e infradotada en las Naciones Unidas, esta organización, por lo menos, va en dirección correcta.

¿Contratar a piratas?

El periodista, Misha Glenny, ha entrevistado a varios de los delincuentes cibernéticos. No sólo ha descubierto que las instituciones encargadas de mantenernos a salvo de los delitos cibernéticos, hacen un trabajo deficiente para disuadir, encontrar e investigar los casos sino que también pueden retrasar la clave de una solución.[8] La evaluación de Glenny es que tenemos un superávit de tecnología que está siendo lanzada al problema pero tenemos una escasez de inteligencia humana. Mientras seguimos vertiendo miles de millones de dólares en soluciones super tecnológicas para la seguridad cibernética, él propone, en su lugar, que estudiemos las características y capacidades de los piratas en el núcleo del problema. Si bien el pirata solo es una pieza de la amenaza contra la seguridad cibernética, en general, esta pieza puede ser la más vulnerable. Muchas figuras en el negocio de la piratería no son mafiosos que desean darse la gran vida, sino genios matemáticos tímidos y socialmente torpes que, en su opinión, están propensos a ser influenciados por patrocinadores más sofisticados que ellos. Glenny, presenta algunos hechos con respecto a varios delincuentes cibernéticos recientemente conocidos, incluyendo al escocés Gary McKinnon, el ucraniano Dimitry Golubov, Renukanth Subramaniam de Sri Lanka, el estadounidense Max Vision, el nigeriano Adewale Taiwo y el turco Cagatay Evyapan. Describe algunas cualidades comunes que comparten ellos y muchos otros piratas. Estos incluyen conocimientos avanzados de matemáticas y ciencias junto con destrezas desarrolladas durante su infancia y temprana adolescencia para piratear computadoras avanzadas antes de que su brújula moral se desarrollara. Además, curiosamente señala las características constantes con el síndrome de Asperger, una forma leve de autismo, así como su depresión concomitante. Estas discapacidades en el mundo real, a menudo, parecen acompañar increíbles habilidades en el mundo virtual de la piratería informática. Al elegir enjuiciar y castigar en lugar de conquistar y contratar a estos genios, Estados Unidos está castigándose y alienando su mejor oportunidad de encontrar y arreglar los problemas que le asechan, o que dice que le asechan. Glenny convincentemente alega que, a veces, deberíamos, más bien, considerar contratarlos —como lo hacen nuestros adversarios. China, Rusia y otros países, afirma, reclutan y contratan gente talentosa antes y después de su participación en delitos cibernéticos. Estos países los contratan para que trabajen para el Estado, mientras nosotros seguimos dependiendo de nuestro sistema de justicia criminal para investigarlos y enjuiciarlos.[9]

¿Tiene un plan de respaldo?

El ingeniero en informática, desde hace mucho tiempo, Danny Hillis, advirtió, a principios de 2013, que mientras gastamos una gran cantidad de energía y atención en la protección de las computadoras en Internet, nos preocupamos poco de la seguridad de Internet como un medio en sí.[10] Hillis considera Internet un sistema emergente. Dice que no la

comprendemos a cabalidad, como las condiciones meteorológicas y la economía: "está cambiando tan rápidamente que incluso los expertos no saben exactamente lo que está pasando."[11] Hillis dice que debido a cómo Internet se ha expandido, aún desconocemos cómo un ataque eficaz de negación de servicio nos afectaría, por lo tanto necesitamos "un plan B."[12]

La buena noticia es que un sistema de respaldo que consiste en un plan básico para servicios esenciales de formas alternativas para que puedan continuar comunicándose y funcionando debe ser relativamente fácil de diseñar, según Hillis.[13] Si bien no ofrece detalles sobre cómo dicho plan podría funcionar, los planificadores de seguridad cibernética quienes estaban trabajando durante el gran susto del año 2000 (refiriéndose a los esperados efectos perjudiciales del bug del Milenio Y2K) podrían desempolvar su viejo plan. El mismo proporcionaría un comienzo adecuado. Los planes de respaldo variarían según el sector de la infraestructura involucrada. El contar con planes de continuidad independientemente de las operaciones basadas en computadoras y, regularmente puestos en práctica y actualizados, puede proporcionar una salvaguardia en caso de que suceda lo peor. Además, los planes pueden ser vehículos para la solución creativa de problemas en una organización. La mentalidad de resiliencia en el centro de las recientes iniciativas del Ejército para mejorar el acondicionamiento general del soldado, puede ponerse en práctica en nuestra infraestructura crítica nacional así como en nuestra salud mental personal. El desarrollar sectores de infraestructura clave bien equilibrados, robustos y seguros cuya resistencia y bienestar total les permita prosperar en una época de gran intercambio de información y persistente amenaza, no es tan difícil de hacer. De hecho, es una meta que vale la pena y que podemos alcanzar.

(Ejército de EUA, Sgto. Candice Harrison)

El Sargento Kenneth Tecala, un Sargento de operaciones aéreas y el Oficial técnico 2° Ben Carmichael, integrador del sistema de mando y control, ambos con la Administración de Artillería de Defensa Aérea, Elemento de Aviación de Brigada, Cuartel General del Equipo de Combate de la 2ª Brigada, 1ª División blindada, arreglan el sistema de Aviso de Cohete, Artillería y Mortero durante la 13.1 Evaluación de Integración de Red en el polígono McGregor, estado de Nuevo México, 13 de noviembre de 2012.

Definitivamente tarde para la fiesta

El que podamos o no evitar un ataque cibernético catastrófico, o por cuánto tiempo, sigue siendo algo incierto. Dada la naturaleza de la amenaza, la vulnerabilidad omnipresente de Internet y de nuestras computadoras y los

recursos limitados de los "buenos", nuestras posibilidades de éxito pueden parecer escasas. Sin embargo, los que trabajamos en el gobierno y los militares hemos estado conscientes de los asuntos de seguridad cibernética durante mucho tiempo. Llevamos a cabo la capacitación anual en línea obligatoria para demostrar nuestro conocimiento sobre la seguridad informática y de información. De hecho, para el personal militar, esas sesiones, a veces, parecen como si el viejo SIGO tomara venganza por todas las cenas formales del pasado. Por lo tanto, podemos enfrentar la seguridad cibernética y esperar que el personal militar esté receptivo para prever y superar los retos de este apresto, de no estar lo suficientemente preparados para hacer frente a una crisis de seguridad cibernética. El informe de 2013 del director de Inteligencia Nacional fue un hecho significativo y un toque de clarín (la actualización de 2014 todavía pone en primer lugar las amenazas cibernéticas). Así como la seguridad física es una responsabilidad inherente y no solamente el trabajo del jefe de la Policia Militar, tampoco la seguridad cibernética es responsabilidad del técnico de cables; es responsabilidad de todos nosotros. Para todo aquel, que erróneamente haya marcado la seguridad cibernética en la casilla de SIGO, debería llamar a su oficina. El podio es nuestro, y SIGO es cada uno de nosotros.

Referencias Bibliográficas

1. Director of National Intelligence James R. Clapper, statement for the record to the Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (12 March 2013), https://www.hsdl.org/?view&did=732599.

2. Mikko H. Hypponen, *Three Types of Online Attack* (November 2011), video online at Technology, Entertainment, and Design (TED) website, http://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack.html.

3. Ralph Langner, *Cracking Stuxnet, a 21st-century Cyber Weapon* (February 2011), video online at Technology, Entertainment, and Design (TED) website, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon; Kaspersky Lab website, Resource 207: *Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected* (11 June 2012), http:// www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

4. Ann Flaherty, "Feds Roll Out Cyber Plan as Hill Vows Legislation," Associated Press, *The Big Story* (13 February 2013), http://bigstory.ap.org/article/white-house-revealing-obamas-cybersecurity-plan.

5. Mike Rogers, "America is Losing the Cyber War vs. China," originally in *Detroit News*, 8 February 2013, reproduced online by Congressman Mike Rogers, http://mikerogers.house.gov/news/documentsingle.aspx?DocumentID=319502.

6. President, Executive Order no. 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* (12 February 2013), https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructurecybersecurity.

7. United Nations Interregional Crime and Justice Research Institute website, About UNICRI, http://web2012.unicri.it/institute/.

8. Misha Glenny, *Darkmarket: How Hackers Became the New Mafia* (New York: Vintage Books, 2012), 271.

9. Ibid., 269.

10. Danny Hillis, *The Internet Could Crash. We need a Plan B* (February 2013), video online at Technology, Entertainment, and Design (TED) website, http://www.ted.com/talks/danny_hillis_the_Internet_could_crash_we_need_a_plan_b.html.

11. Ibíd.

12. Ibíd.

13. Ibíd.