(Foto: Associated Press, Khalil Senosi)

Amina Harun habla por teléfono celular mientras vende sandías en el mercado de frutas y hortalizas más grande en Nairobi, Kenia, 26 de julio de 2005. Las empresas de teléfonos celulares que se establecieron en África hace más de una década hoy en día incluyen agricultores, pescadores pobres e incluso desempleados como abonados. Algunos investigadores incluso colocan teléfonos celulares en elefantes para rastrear sus movimientos.

La seguridad cibernética de las naciones anfitrionas en las operaciones de estabilización futuras

Mención honorífica, Competencia DePuy de 2015

Mayor Michael Kolton, Ejército de EUA

Hoy en día, el ciberespacio es fundamental en la gobernabilidad, crecimiento económico y vidas sociales de las poblaciones que viven en países desarrollados y en vías de desarrollo. Además, las capacidades de ciberespacio han resultado ser indispensables en los esfuerzos de socorro en casos de desastre y zonas de conflicto. Mientras tanto, los adversarios también se han desarrollado en su sofisticación y ahora amenazan cada vez más las capacidades del ciberespacio.

Puesto que las organizaciones no militares retienen experiencias significativas en la seguridad cibernética y protección de infraestructura crítica, las mejores prácticas que estas organizaciones han desarrollado proporcionan un marco para la futura doctrina del Ejército. En el presente artículo, se analiza la integración de tales precedentes para la seguridad cibernética de las naciones anfitrionas en las operaciones de estabilización del Ejército de EUA.

Cómo definir el ciberespacio

En su definición del ciberespacio, los expertos de seguridad Peter Singer y Allan Friedman expresan en términos sencillos: «En esencia, el ciberespacio es el dominio de las redes computacionales (y los usuarios de las mismas) en las cuales la información es guardada, compartida y comunicada en línea»[1]. De igual manera, las Fuerzas Armadas de EUA definen el ciberespacio como «el dominio global dentro del ambiente de información que consta de infraestructuras de tecnología de información en redes interdependientes y datos residentes, incluyendo la Internet, redes de telecomunicaciones, sistemas computarizados, además de procesadores y controladores integrados»[2]. En los siguientes treinta años, el Ejército anticipa que los conflictos se harán más complejos a medida que los adversarios hagan uso de tecnologías avanzadas, incluyendo las que colocan la lucha en el dominio cibernético[3].

Con respecto a la defensa del territorio nacional, las Fuerzas Armadas de EUA han invertido en las capacidades cibernéticas «para proteger redes e infraestructura críticas»[4]. El Pentágono ha concentrado los esfuerzos de seguridad cibernética en la protección de sistemas militares[5]. La doctrina actual sobre el ciberespacio militar enfatiza proteger los sistemas de información de las fuerzas armadas para garantizar la libertad de maniobra[6].

El Ejército, el ciberespacio y las operaciones de estabilización

La doctrina actual no aborda adecuadamente los imperativos del ciberespacio para las operaciones de estabilización. Y, puesto que aun los países más pobres del mundo —las áreas más probables en las cuales operaciones militares de EUA serán realizadas con socios de coalición en el futuro— hoy en día dependen del ciberespacio, en la doctrina militar de EUA deben considerarse las maneras que el ciberespacio simultáneamente incide en todas las líneas de esfuerzo en las operaciones de estabilización.

Estados Unidos espera que sus fuerzas armadas se preparen para las operaciones de estabilización y las ejecuten sin importar el nivel de incertidumbre en el ambiente de información. Las operaciones de estabilización incluyen «varias misiones, tareas y actividades militares realizadas fuera de Estados Unidos en coordinación con otros instrumentos de poder nacional para mantener o restablecer un ambiente seguro, proporcionar servicios gubernamentales básicos, reconstrucción de infraestructura de emergencia y socorro humanitario»[7]. Es importante notar que todas las operaciones conjuntas dependen del ciberespacio, lo que permite que la fuerza conjunta integre sus operaciones en todas las zonas terrestres, aéreas, marítimas y espaciales[8]. Consecuentemente, el Ejército también debe prepararse para posiblemente lograr la seguridad cibernética de una nación anfitriona en las operaciones de estabilización.

Las redes de comunicaciones inalámbricas y móviles: Los ejemplos de un servicio básico que depende del ciberespacio

Un ejemplo del ciberespacio es la red civil de comunicaciones inalámbricas y móviles. Las crisis recientes han demostrado que tales redes móviles son indispensables para los servicios de emergencia. Por ejemplo, durante el brote de ébola en 2014, el gobierno de Sierra Leona usó mensajes de texto para transmitir mensajes de salud pública[9]. El compartimiento de datos móviles también fue esencial en los esfuerzos de recuperación después de los terremotos en Haití y Chile en 2010[10]. Y, después del terremoto en Nepal en 2015, las redes móviles permitieron comunicaciones decisivas entre wl personal de asistencia humanitaria y la población del

lugar. Con las líneas telefónicas abrumadas, los sobrevivientes nepaleses dependieron de la Internet para compartir la información[11].

Las redes móviles de nuevo resultaron ser indispensables durante la respuesta al desastre del terremoto y el tsunami de 2011 en Japón, cuando la población del lugar dependió en gran medida de las redes móviles para acceder a información crítica de emergencia[12]. Esta dependencia también fue ejemplificada después del atentado explosivo del Maratón de Boston en 2013 y el terremoto de 2007 en San Francisco cuando ciudadanos ansiosos abrumaron las redes móviles con una oleada masiva de comunicaciones[13].

Después de que el tifón Haiyan golpeó las Filipinas en 2013, los habitantes y organizaciones benéficas tuvieron dificultades para restaurar el servicio móvil[14]. En las operaciones de socorro, Kristalina Georgieva, la Comisaria de Cooperación Internacional, Ayuda Humanitaria y Respuesta a las Crisis de la Unión Europea (EU), dijo «Lo primero [prioritariamente] es acceder a las áreas remotas lo más pronto posible y el asunto de acceso se refiere tanto al transporte como a la restauración de las telecomunicaciones»[15].

Antes de que el tifón Haiyan tocara tierra, la Groupe Speciale Mobile Association (GSMA) desplegó un equipo de respuesta a desastres para apoyar al gobierno filipino y las empresas de telecomunicaciones del país en la ubicación de sus esfuerzos de respuesta[16]. La GSMA es un organismo de la industria que representa a más de 250 empresas de telecomunicaciones tales como AT&T, Orange, Telenor, Verizon y Vodafone[17]. Después de que el tifón golpeara, los representantes de la GSMA ayudaron a restaurar las redes de intercambio de información para posibilitar servicios básicos tales como dinero móvil (el uso de dispositivos como teléfonos móviles para enviar dinero en lugar de efectivo)[18].

La GSMA explica, «los dispositivos móviles frecuentemente son una de las primeras cosas que las personas agarran cuando ocurre un desastre; por ejemplo, una de las primeras solicitudes por los desplazados en la montaña Sinjar en Irak fue un medio para recargar sus teléfonos móviles para poder obtener información, sobre sus seres queridos, y tomar parte en los esfuerzos de respuesta»[19]. Estos ejemplos demuestran que, ya para 2015, las redes móviles verdaderamente se habían convertido en un componente indispensable de gestión de crisis.

Más allá de las comunicaciones directas, los teléfonos móviles también han posibilitado las actividades bancarias móviles. Desde enero de 2015, 38 por ciento de la población mundial vivía sin acceso a una cuenta bancaria; las actividades bancarias móviles prometen ser la vía principal para estas comunidades[20]. Por ejemplo, la institución financiera más grande de Pakistán es un proveedor de telecomunicaciones móviles noruego[21]. En otro ejemplo, Kenia ostenta uno de los sistemas de pagos por teléfono móvil más populares y exitosos en el mundo[22].

Sin embargo, en un informe de 2011, el Equipo de Preparación para Emergencias Computarizadas del Departamento de Seguridad del Territorio Nacional (DHS) de EUA advirtió que «cada vez más, los teléfonos móviles cobran más valor como blancos de ataques»[23]. Los profesionales de seguridad cibernética consideran los dispositivos móviles la mayor vulnerabilidad de sus redes[24]. Entre agosto de 2013 y marzo de 2014, los ataques mensuales contra los dispositivos móviles incrementaron más de 800 por ciento[25]. En un caso, criminales cibernéticos chinos usaron falsas aplicaciones falsas bancarias móviles para engañar a los usuarios e inducirlos a que entraran sus credenciales, permitiendo que los piratas informáticos (hackers) robaran millones de dólares[26]. Puesto que las comunidades en conflictos futuros dependerán de bancas móviles, las amenazas cibernéticas a las últimas incidirán en las operaciones de estabilización del Ejército.

Cómo proteger y restaurar servicios básicos que dependen del ciberespacio

La comunidad internacional juega un rol crítico en apoyo a los esfuerzos de restauración de las telecomunicaciones como un servicio básico para las partes interesadas. La Unión Internacional de Telecomunicaciones (ITU) tiene un mandato de las Naciones Unidas para gestionar las tecnologías de la información y la comunicación (ICT). Los miembros de la ITU incluyen 173 gobiernos, centenares de instituciones no gubernamentales y empresas privadas[27]. En el primer trimestre de 2015, el personal de la ITU se desplegó para apoyar la restauración de las telecomunicaciones en los esfuerzos de socorro en Malaui, Mozambique, Micronesia, Nepal y Vanuatu[28]. Los esfuerzos en el campo de las telecomunicaciones representan un imperativo más amplio para el crecimiento de la ICT en el área de estabilización.

(Foto: 1ª Ala de Operaciones Especiales, Sgto. 2º Ryan Whitney)

Integrantes de las fuerzas armadas de Ucrania monitorean y mantienen el acceso a la red durante el ejercicio Combined Endeavor 2011 en Grafenwoehr, Alemania, 19 de septiembre de 2011. Combined Endeavor, un ejercicio anual que incluye casi cuarenta socios de la OTAN, Partnership for Peace [Asociación para la paz] y de la comunidad de seguridad estratégica, está concebido para incrementar la interoperabilidad y mejorar los procesos de comunicaciones entre las naciones participantes.

La paradoja del ciberespacio y ejemplos de amenazas emergentes

La protección y restauración de las ICT son componentes necesarios de la prosperidad[29]. El crecimiento económico futuro dependerá de la movilidad y flexibilidad de las redes de un país[30]. En 2007, la ITU enfatizó, «Las organizaciones y países necesitan concentrarse en las capacidades de innovación y la adaptabilidad rápida, respaldadas por un sistema de información fuerte y seguro, si desean sobrevivir y hacerse valer como actores de largo plazo en el nuevo entorno competitivo»[31]. Un mayor nivel de acceso a la Internet, servicios móviles y banda ancha impulsa el crecimiento económico[32]. Además, el Banco Mundial identifica las ICT como factores clave en el desarrollo social[33]. Mientras los países en vías de desarrollo continúan profundizando la penetración de sus ICT, disminuyen sus costos de infraestructura a largo plazo, creando así un ciclo virtuoso[34]. Los costos decrecientes impulsan aún más la penetración de banda ancha[35]. En suma, las ICT desencadenan fuerzas económicas latentes en las economías en vías de desarrollo[36].

En un informe de 2014, los investigadores de Microsoft describieron una «paradoja de seguridad cibernética» que los países en vías de desarrollo enfrentan con una baja penetración de las ICT[37]. Estos países sufren las tasas más altas de infección de programas malignos. Además, mientras estos países desarrollan infraestructuras de ICT, aceleran sus tasas de infección[38]. Por lo tanto, los países más pobres con los niveles de ICT más bajos pueden ser los más vulnerables a las amenazas de seguridad cibernética.

Dado que las zonas de conflicto ya sufren de niveles elevados de tráfico de personas, explotación de niños, narcotráfico y crimen organizado, el ciberespacio vulnerable hace de ellas blancos fáciles para la explotación[39]. Por lo tanto, el crimen cibernético se ha convertido en una evolución inevitable para viles actores en estas

circunstancias. Por ejemplo, después del terremoto de 2010 en Haití, los criminales cibernéticos inmediatamente publicaron portales de Internet para instituciones benéficas falsas a fin de engañar a donantes[40].

En otras partes, los ataques cibernéticos se han convertido en un componente del conflicto político. Por ejemplo, cuando Rusia tomó control de Crimea en 2014, los usuarios de teléfonos móviles en Ucrania sufrieron una interrupción de servicio significativa[41]. Y, durante la elección presidencial de mayo de 2014 en Ucrania, hackers pro-rusos penetraron el sistema de votación electrónica e instalaron un código maligno capaz de borrar un gran número de votos[42].

En respuesta, en febrero de 2015, el gobierno ucranio en Kiev publicó una nueva estrategia de seguridad cibernética que establece «un registro nacional de objetos cruciales de la infraestructura nacional de IT, con la meta de garantizar su protección»[43]. A pesar de estos esfuerzos, un supuesto ataque cibernético el 23 de diciembre de 2015 dejó a más de setecientos mil ucranios sin electricidad[44]. La experiencia de Ucrania demuestra la relevancia de la seguridad cibernética en las operaciones de estabilización.

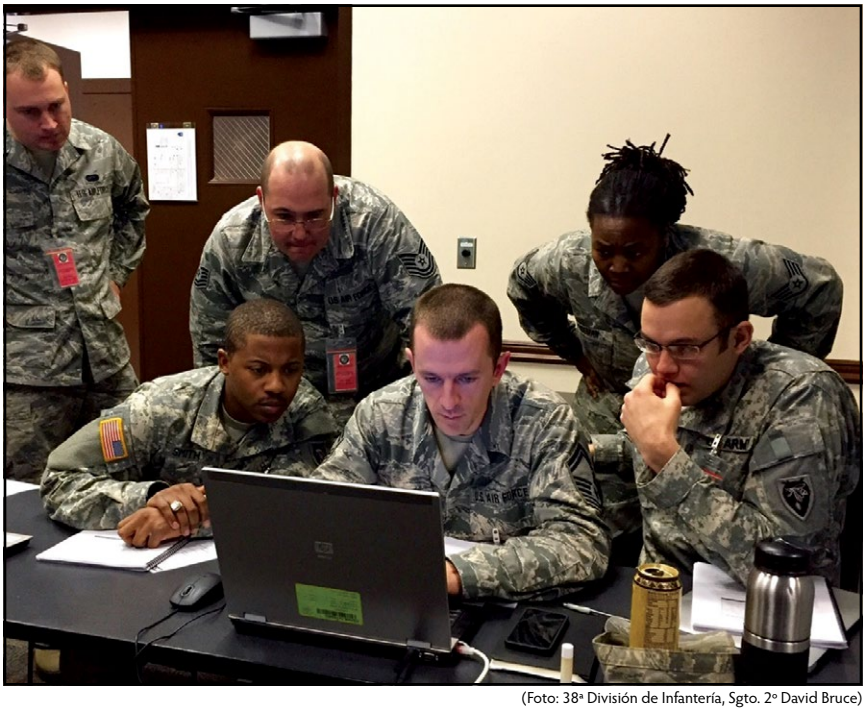
Alianzas públicas-privadas

Parecido a Kiev, Estados Unidos continúa refinando la política de seguridad cibernética y protección de la infraestructura crítica (CIP) para adaptarse a las amenazas emergentes. La infraestructura crítica, como es definida en la Directiva Presidencial de Política 21, son «sistemas y medios, ya sean físicos o virtuales, tan vitales para Estados Unidos que la incapacidad o destrucción de tales sistemas y medios tendría un impacto debilitante en la seguridad, la seguridad nacional económica, la seguridad o salud pública nacional o cualquier combinación de estos sectores»[45]. Estados Unidos clasifica la infraestructura crítica en dieciséis sectores, desde la energía hasta el transporte.

La discusión de la protección de la infraestructura crítica, así como las implicaciones y cambios de política que han resultado, ha surgido en los últimos veinte años. En 2002, el DHS asumió un rol de vanguardia en la protección de la infraestructura crítica[46]. Aún antes de esto, la Orden Ejecutiva (EO) del presidente Bill Clinton 13010, firmada en 1996, clasificó las amenazas a la infraestructura crítica como físicas y cibernéticas[47]. Casi dos décadas después, en la *Quadrennial Homeland Security Review* [Revisión Cuadrienal de Seguridad del Territorio Nacional], se hizo hincapié en los grandes efectos destructivos posibles de las amenazas cibernéticas a la infraestructura crítica[48].

La necesidad de cooperación gubernamental, militar y civil en la protección del ciberespacio

El aspecto central de la seguridad cibernética eficaz y protección de la infraestructura crítica es la colaboración pública-privada. En 2013, la EO 13636 del presidente Barack Obama mejoró la seguridad cibernética



(Foto: 38ª División de Infantería, Sgto. 2º David Bruce)

Más de 350 soldados de la Guardia Nacional, aerotécnicos y civiles de 42 estados se reunieron en el Campamento Atterbury, estado de Indiana, para participar en el ejercicio Cyber Shield [Escudo cibernético], de 9 a 20 de marzo de 2015. La intención fue adiestrar a los participantes en cómo defender infraestructura crítica contra ataques cibernéticos. El ejercicio incluyó una competencia en que 24 equipos lucharon en el ciberespacio para proteger las computadoras y sistemas de control industriales relacionados de una ciudad ficticia contra adversarios maliciosos y altamente calificados. Un equipo combinado de los estados de Oregón e Idaho ganó la competencia.

para la protección de infraestructura crítica a través de la colaboración pública-privada y ordenó al Instituto Nacional de Estándares y Tecnología (NIST) que desarrollara «un marco para disminuir los riesgos cibernéticos a la infraestructura crítica»[49]. En 2014, El NIST publicó un marco preliminar que afirmó la cooperación pública-privada en la seguridad cibernética[50].

Singer y Friedman destacan, «el sector privado controla aproximadamente el 90 por ciento de la infraestructura crítica de EUA, y estas empresas usan el ciberespacio para, entre otra cosas, equilibrar los niveles de cloración en el agua de su ciudad, controlar el flujo de gas que calienta su hogar y ejecutar las transacciones financieras que mantienen estable los precios de divisas»[51]. El subsecretario de seguridad cibernética y comunicaciones del DHS Andy Ozment explica, «No hay manera de que el gobierno pueda ayudar a todas las empresas en Estados Unidos a protegerse»[52]. La cooperación pública-privada es fundamental para desarrollar un marco adaptable de seguridad cibernética[53].

En 1998, la Directiva Presidencial de Política (PPD)-63 estableció los Centros de Intercambio y Análisis de Información (ISAC), que invitan a las partes interesadas del sector privado a desarrollar redes para intercambiar las mejores prácticas y facilitar respuestas a las crisis[54]. Los ISAC dependen de la industria privada para llevar a cabo «misiones no regulatorias y no policiales»[55]. Estos son «centros coordinadores de información en/entre varios sectores y proporcionan una colección de datos históricos que será usada por el sector privado, y dependiendo de cuán adecuado lo considere el ISAC, por el gobierno»[56]. Desde 1998, el modelo del ISAC se ha desarrollado para facilitar la cooperación entre los gobiernos a nivel federal, estatal, local, tribal y territorial.

En 2013, la PPD-21 ordenó el establecimiento de dos centros nacionales por el DHS para gestionar la protección de infraestructura física y cibernética[57]. El DHS incorporó esta orientación en su National Infrastructure Protection Plan[58]. El Centro Nacional de Coordinación de Infraestructura gestiona el dominio físico y el Centro Nacional de Seguridad Cibernética e Integración de Comunicaciones (NCCIC) administra el dominio cibernético[59]. Estos centros de coordinación también facilitan la colaboración pública-privada a través de los ISAC.

En febrero de 2015, la EO 13691 ordenó al DHS a desarrollar las Organizaciones de Intercambio y Análisis de Información (ISAO)[60]. Estas organizaciones extienden el modelo de ISAC más allá de los dieciséis sectores críticos de infraestructura a otros sectores de alto valor tales como despachos de abogados y empresas de contabilidad, que son blancos primarios de ataques cibernéticos[61]. La EO 13691 ordena que el NCCIC supervise los cursos de acción de las ISAO[62]. A pesar de estar en sus comienzos, las ISAO intentan cooperar a pesar de la desconfianza y fricción entre el gobierno y otras partes interesadas. Este tipo de malabarismo es paralelo con el futuro ambiente de información del Ejército y tiene un gran impacto en la conducción de las operaciones de estabilización del Ejército.

Conclusión

Según la doctrina, las operaciones de estabilización requieren coordinación con el gobierno de la nación anfitriona, la industria comercial, los socios multinacionales e incluso las fuentes no gubernamentales. Esta mentalidad cooperativa es relevante para las operaciones del ciberespacio. Dado que los gobiernos dependen del ciberespacio para proporcionar los servicios básicos, la seguridad cibernética requiere una línea de esfuerzo que apoye simultáneamente las otras cinco tareas de las operaciones de estabilización identificadas en la Publicación de Doctrina del Ejército 3-07, *Stability*:[63]

- Establecer la seguridad civil
- Establecer el control civil
- Restaurar los servicios básicos
- Apoyar la gobernabilidad
- Apoyar el desarrollo económico e infraestructura
- *Proteger la infraestructura del ciberespacio*

En la doctrina del ciberespacio, el Estado Mayor Conjunto destaca la importancia de integrar las iniciativas cibernéticas con otras partes interesadas. En su publicación *Cyber Strategy* [Estrategia cibernética] de 2015, el Departamento de Defensa describió «el desarrollo de alianzas, coaliciones y asociaciones» como una actividad fundamental de la seguridad cibernética[64]. En un memorándum publicado en junio de 2015, el almirante Michael Rogers escribió, «las operaciones en el ciberespacio exigen niveles sin precedentes de colaboración e intercambio de información conjunta, interinstitucional y de coalición y, por lo tanto, seguiremos siendo socios confiables cuando colaborems con

otras agencias, con aliados y amigos en el exterior y con el mundo académico»[65]. El Estado Mayor Conjunto ha identificado obstáculos profundos en la cooperación pública-privada en cuanto a las alarmas de seguridad cibernética.

> Muchas organizaciones no gubernamentales son renuentes a asociarse con organizaciones militares en cualquier tipo de relación formal, especialmente en los casos donde se realizan CO [operaciones cibernéticas], porque hacerlo podría comprometer su estatus como entidad independiente, restringiría su libertad de movimiento y aun pondría en riesgo a sus miembros en ambientes ambiguos u hostiles permisibles[66].

En el desarrollo del modelo ISAC/ISAO, sus arquitectos han buscado superar dicha desconfianza entre el gobierno, el sector industrial y las organizaciones no gubernamentales. Si bien de ninguna manera es una panacea, el modelo de ISAC/ISAO ofrece al Ejército un marco para facilitar la cooperación en las operaciones de estabilización en el futuro.

Esto es un imperativo operativo tanto actual como futuro. Según venga al caso, el Ejército debe estar preparado para restaurar la seguridad cibernética de la infraestructura crítica de una nación anfitriona, coordinando esfuerzos con organizaciones intergubernamentales tal como la Unión Internacional de Telecomunicaciones, la industria privada tales como los miembros de la Groupe Speciale Mobile Association y varias organizaciones gubernamentales. A fin de facilitar la colaboración necesaria, el modelo de ISAC/ISAO proporciona un punto de partida para las operaciones futuras. ■

El mayor Michael Kolton, Ejército de EUA, es estudiante de posgrado en el Instituto de Asuntos Internacionales de la Universidad de Yale. Kolton es un oficial especialista de área, especializado en China. Previamente ha servido en calidad de oficial de infantería con despliegues en Irak y Afganistán. Cuenta a su haber con una maestría en Ciencias Económicas de la Universidad de Hawái en Manoa y una licenciatura en Ciencias Económicas de la Academia Militar de EUA en West Point, Nueva York.

Referencias bibliográficas

1. Peter W. Singer y Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Londres: Oxford University Press, 2014), p. 13.

2. Joint Publication (JP) 3-12(R) *Cyberspace Operations* (Washington, DC: U.S. Government Printing Office [GPO], 5 de febrero de 2013), v.

3. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World, 2020-2040* (Fuerte Eustis, Virginia: TRADOC, 31 de octubre de 2014), p. 11.

4. Joint Chiefs of Staff, National Military Strategy of the United States 2015, junio de 2015, p. 7, accedido 11 de diciembre de 2015, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

5. Ibíd., págs. 4 y 11.

6. JP 3-12(R), *Cyberspace Operations*, v; Gregory Conti, John Nelson y David Raymond, «Towards a Cyber Common Operating Picture» (presentado en la 5ª Conferencia Internacional sobre el Conflicto Cibernético, Tallinn, Estonia, de 4 a 7 de junio de 2013), vi.

7. JP 3-07, *Stability Operations* (Washington, DC: U.S. GPO, 29 de septiembre de 2011), vii.

8. JP 3-12 (R), *Cyberspace Operations*.

9. «Ebola in Sierra Leone: Which Doctor?» *Economist*, 19 de junio de 2014, accedido 14 de diciembre de 2015, http://www.economist.com/blogs/baobab/2014/06/ebola-sierra-leone.

10. «Online Crisis Management: A Web of Support», *Economist*, 14 de julio de 2011, accedido14 de diciembre de 2015, http://www.economist.com/blogs/babbage/2011/07/online-crisis-management.

11. John Ribeiro, «Internet Becomes a Lifeline in Nepal after Earthquake», *Computer World*, 25 de abril de 2015, accedido 14 de diciembre de 2015, http://www.computerworld.com/article/2914641/internet/internet-becomes-a-lifeline-in-nepal-after-earthquake.html.

12. «Dealing with Japan's Disaster: The Information Equation», *Economist*, 24 de abril de 2011, accedido 14 de diciembre de 2015, http://www.economist.com/blogs/babbage/2011/04/dealing_japans_disaster.

13. Neal Ungerleider, «Why Your Phone Doesn't Work During Disasters—And How to Fix It», *Fast Company*, 17 de abril de 2013, accedido 14 de diciembre de 2015, http://www.fastcompany.com/3008458/tech-forecast/why-your-phone-doesnt-work-during-disasters-and-how-fix-it.

14. «The CDAC Network: Typhoon Haiyan Learning Review», Communicating with Disaster Affected Communities (CDAC) Network, de noviembre de 2014, 20, accedido 22 de

diciembre de 2015, http://www.cdacnetwork.org/contentAsset/raw-data/7825ae17-8f9b-4a05-bfbd-7eb9da6ea8c1/attachedFile.

15. «Typhoon Haiyan: Philippines Destruction "Absolute Bedlam"» BBC News, 11 de noviembre de 2013, accedido 14 de diciembre de 2015, http://www.bbc.com/news/world-asia-24894529.

16. Serena Brown, «The Private Sector: Stepping Up», Humanitarian Exchange Magazine 63 (enero de 2015), accedido 1 de junio de 2015, http://www.odi-hpn.org/humanitarian-exchange-magazine/issue-63/the-private-sector-stepping-up.

17. «Brief History of GSM & the GSMA», sitio web de la Groupe Speciale Mobile Association, accedido 22 de diciembre de 2015, http://www.gsma.com/aboutus/.

18. «About the Mobile Money Programme», sitio web de la Groupe Speciale Mobile Association, accedido 23 de diciembre de 2015, http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/about.

19. «GSMA Launches Humanitarian Connectivity Charter», comunicado de prensa de la Groupe Speciale Mobile Association, 2 de marzo de 2015, accedido 22 de diciembre de 2015, http://www.gsma.com/newsroom/press-release/gsma-launches-humanitarian-connectivity-charter/.

20. Asli Demirguc-Kunt y col., «The Global Findex Database 2014: Measuring Financial Inclusion around the World», World Bank Policy Research Working Paper 7255, abril de 2015, accedido 14 de diciembre de 2015, http://documents.worldbank.org/curated/en/2015/04/24368699/global-findex-database-2014-measuring-financial-inclusion-around-world.

21. «Global Trends in Mobile Banking», Papel blanco de la IGATE Corporation, 2014, 2, accedido 14 de diciembre de 2015, http://www.igate.com/documents/11041/100349/Global_trends_in_Mobile_Banking.pdf/cf246d31-83c6-44b8-b6fb-a43f38ca2633.

22. Ibíd.

23. Paul Ruggiero y Jon Foote, «Cyber Threats to Mobile Phones», informe para U.S. Computer Emergency Readiness Team, preparado por la Universidad Carnegie Mellon, 2011, accedido 22 de diciembre de 2015, https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf.

24. «2014 Cyberthreat Defense Report: North America & Europe», CyberEdge Group, 2014, 5, accedido 22 de diciembre de 2015, http://cyber-edge.com/wp-content/uploads/2014/01/CyberEdge-2014-CDR.pdf.

25. «Mobile Cyber Threats», Kaspersky Lab and INTERPOL Joint Report, October 2014, 13, accedido 22 de diciembre de 2015, http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf.

26. Pierluigi Paganini, «Yanbian Gang Steals Millions from Mobile Banking Customers of South Korea», *Security Affairs*, 18 de febrero de 2015, accedido 22 de diciembre de 2015, http://securityaffairs.co/wordpress/33709/cyber-crime/yanbian-gang-mobile-banking.html.

27. «ITU Disaster Response», sitio web de ITU, abril 2015, accedido 22 de diciembre de 2015, http://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Response.aspx.

28. Ibíd.

29. Alessandra Colecchia y Paul Schreyer, «ICT Investment and Economic Growth in the 1990s: Is the United States a Unique Case? A Comparative Study Nine OECD Countries», *OECD Science, Technology and Industry Working Papers*, julio de 2001, p. 4, http://www.oecd-ilibrary.org/docserver/download/5lgsjhvj7mbs.pdf?expires=1450121640&id=id&accname=guest&checksum=1C2F491CF06E94F3FB8FA47AD9E158C7.

30. «Friends and Forecasters: Ten Thoughts for the Future», *Economist*, 17 de diciembre de 2013, accedido 14 de diciembre de 2015, http://www.economist.com/blogs/theworldin2014/2013/12/friends-and-forecasters.

31. *Cybersecurity Guide for Developing Countries* (Ginebra: Telecommunication Development Bureau, 2007), p. 7.

32. Christine Zhen-Wei Qiang, «Mobile Telephony: A Transformational Tool for Growth and Development», *Private Sector Development* 4 (noviembre de 2009).

33. Mark D. J. Williams, «Advancing the Development Backbone Networks in Sub-Saharan Africa», *Information and Communications for Development 2009: Extending Reach and Increasing Impact* (Washington, DC: World Bank, 2009), p. 4, accedido 22 de diciembre de 2015, http://siteresources.worldbank.org/EXTIC4D/Resources/5870635-1242066347456/IC4D_2009_Chapter4.pdf.

34. Ibíd.

35. «ICT Facts and Figures», sitio web de International Telecommunication Union, febrero 2013, accedido 22 de diciembre de 2015, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf.

36. «The Role of Wi-Fi in Developing Nations», Wireless Broadband Alliance website, 24 de abril de 2014, accedido 22 de diciembre de 2015, http://www.wballiance.com/industryinsights/the-role-of-wi-fi-in-developing-nations/.

37. David Burt y col., «The Cybersecurity Risk Paradox: Impact Social, Economic, and Technological Factors on Rates Malware», Microsoft Intelligence Report Special Edition, 2014, p. 2, accedido 22 de diciembre de 2015, http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity-Risk-Paradox.pdf.

38. Ibíd., p. 8.

39. «Human Trafficking: A Brief Overview», *Social Development Notes Conflict, Crime and Violence* 122 (diciembre de 2009); «UNODC and United Nations Peacekeeping Forces Team Up to Combat Drugs and Crime in Conflict Zones», United Nations Office on Drugs and Crime, 2 de marzo de 2011, accedido 22 de diciembre de 2015, https://www.unodc.org/unodc/en/frontpage/2011/March/unodc-and-dpko-team-up-to-combat-drugs-and-crime-in-conflict-zones.html.

40. Michelle Singletary, «Haiti Earthquake Brings out Generosity, and Scam Artists», *Washington Post*, 17 de enero de 2010, accedido 22 de diciembre de 2015, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/15/AR2010011504692.html.

41. Shane Harris, «Hack Attack: Russia's First Targets in Ukraine: Its Cell Phones and Internet Lines», Foreign Policy, 3 de marzo de 2014, accedido 22 de diciembre de 2015, http://foreignpolicy.com/2014/03/03/hack-attack/.

42. Mark Clayton, «Ukraine Election Narrowly Avoided "Wanton Destruction" from Hackers», *Christian Science Monitor*, 17 de junio de 2014, accedido 25 de febrero de 2015, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

43. Eugene Gerden, «Ukrainian Government to Counter Cyber-Attacks», *SC Magazine: For IT Security Professionals*, 13 de febrero de 2015, accedido 22 de diciembre de 2015, http://www.scmagazineuk.com/ukrainian-government-to-counter-cyber-attacks/article/397970/.

44. James Titcomb, «Ukrainian blackout blamed on cyber-attack», *Telegraph*, 5 de enero de 2016, accedido 6 de enero de 2016, http://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html.

45. Presidential Policy Directive (PPD-21), «Presidential Policy Directive—Critical Infrastructure Security and Resilience», 12 de febrero de 2013, accedido 22 de diciembre de 2015, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

46. Franklin D. Kramer, Stuart H. Starr y Larry Wentz, *Cyberpower and National Security* (National Defense University: Potomac Books, 1 April 2009), p. 132, Kindle edition; Richard White, «Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model», Homeland Security Affairs 10 (1) (febrero de 2014): p. 2, accedido 7 de abril de 2015, https://www.hsaj.org/articles/254.

47. Executive Order 13010, «Critical Infrastructure Protection», 15 de julio de 1996, accedido 22 de diciembre de 2015, http://fas.org/irp/offdocs/eo13010.htm.

48. U.S. Department of Homeland Security, *2014 Quadrennial Homeland Security Review* (QHSR), 18 de junio de 2014, accedido 22 de diciembre de 2015, http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

49. «Foreign Policy: Cybersecurity», sitio web de The White House, accedido 22 de diciembre de 2015, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity; Executive Order 13636, «Improving Critical Infrastructure Cybersecurity», 12 de febrero de 2013, accedido 22 de diciembre de 2015, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

50. «NIST Roadmap for Improving Critical Infrastructure Cybersecurity», National Institute Standards and Technology, 12 de febrero de 2014, accedido 22 de diciembre de 2015, http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

51. Singer y Friedman, *Cybersecurity*, p. 15.

52. Andy Ozment (Assistant Secretary for Cybersecurity and Communications DHS), «Cybersecurity and the Law», American Bar Association, 00:34:53, accedido 22 de diciembre de 2015, http://www.c-span.org/video/?324377-1/discussion-cybersecurity-law.

53. U.S. Government Accountability Office, *Cybersecurity National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, Report to Congressional Addressees*, GAO-13-187 (Washington, DC: U.S. GPO, febrero de 2013), p. 8.

54. Kramer y col., *Cyberpower*, 131; Presidential Decision Directive (PDD-63), «Critical Infrastructure Protection», 22 de mayo de 1998, accedido 22 de diciembre de 2015, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

55. PDD-63, «Infrastructure Protection».

56. Ibíd.

57. PPD-21, «Infrastructure Security and Resilience».

58. «National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience», U.S. Department of Homeland Security, 2013, iv, accedido 22 de diciembre de 2015, https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

59. «Supplemental Tool: Connecting to the NICC and the NCCIC», Supplement to National Infrastructure Protection Plan (NIPP) 2013, U.S. Department of Homeland Security, 2013, 1, accedido 22 de diciembre de 2015, http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Connecting%20to%20the%20NICC%20and%20NCCIC_508.pdf.

60. Executive Order 13691, «Promoting Private Sector Cybersecurity Information Sharing», 13 de febrero de 2015, accedido 22 de diciembre de 2015, http://www.gpo.gov/fdsys/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf.

61. «Information Sharing and Analysis Organizations», Homeland Security (18 de marzo de 2015), accedido 10 de abril de 2015, http://www.dhs.gov/isao.

62. «Information Sharing and Analysis Organizations Public Meeting», transcripciones de ISAO (31 de marzo de 2015), accedido 22 de diciembre de 2015, http://www.dhs.gov/publication/isao-transcripts.

63. Army Doctrinal Publication 3-07, *Stability Operations* (Washington, DC: U.S. GPO, agosto de 2012), p. 11.

64. *Department Of Defense Cyber Strategy* (Washington, DC: Office of the Secretary of Defense, abril de 2015), p. 4.

65. *Beyond the Build: Delivering Outcomes through Cyberspace* (Fuerte Meade, Maryland: US Cyber Command, 3 de junio de 2015), p. 3.

66. JP 3-12 (R), *Cyberspace Operations*, p. IV-15.