(Khalil Senosi, Associated Press)

Vendedora de melancias fala ao celular, na maior feira de frutas e hortaliças de Nairóbi, no Quênia, 26 Jul 05. As empresas de telefonia celular, que se estabeleceram na África há mais de uma década, hoje incluem, entre seus assinantes, pobres agricultores, pescadores e desempregados. Alguns pesquisadores até prendem celulares a elefantes para rastrear seus movimentos.

Menção Honrosa, Concurso DePuy 2015

A Segurança Cibernética do País Anfitrião em Futuras Operações de Estabilização

Maj Michael Kolton, Exército dos EUA

O ciberespaço hoje é fundamental para a governança, o crescimento econômico e as vidas sociais das populações em países desenvolvidos e em desenvolvimento. Além disso, as capacidades cibernéticas se mostraram indispensáveis para esforços de socorro em desastres e em zonas de conflito. Enquanto isso, os adversários também evoluíram em termos de sofisticação, hoje representando, cada vez mais, uma ameaça em capacidades cibernéticas.

Considerando o fato de que organizações não militares detêm considerável experiência na segurança cibernética, ou cibersegurança, e na proteção de infraestrutura crítica, as melhores práticas por elas desenvolvidas fornecem um modelo para a futura doutrina do Exército dos Estados Unidos da América (EUA). Este artigo explora a integração desses precedentes para a segurança cibernética de um país anfitrião durante operações de estabilização do Exército dos EUA.

Definição de Ciberespaço

Os especialistas em segurança Peter Singer e Allan Friedman definem ciberespaço de maneira simples: "Em sua essência, o ciberespaço é o domínio das redes de computadores (e dos usuários por trás deles) em que as informações são armazenadas, compartilhadas e comunicadas *on-line*"[1]. De maneira semelhante, as Forças Armadas dos EUA definem ciberespaço como o "domínio global dentro do ambiente de informações que consiste na rede interdependente de infraestruturas de tecnologia da informação e dados residentes, incluindo a internet, as redes de telecomunicações, os sistemas computacionais e os processadores e controladores embutidos"[2]. O Exército dos EUA prevê que, nos próximos 30 anos, os conflitos se tornarão mais complexos, à medida que os adversários explorarem tecnologias avançadas, incluindo as que levam o combate para o domínio cibernético[3].

Para a defesa interna norte-americana, as Forças Armadas dos EUA têm investido em capacidades cibernéticas "para proteger redes e infraestruturas vitais"[4]. O Pentágono concentra os esforços de segurança cibernética na proteção dos sistemas militares[5]. A atual doutrina cibernética militar enfatiza a proteção dos sistemas de informações próprios das Forças Armadas, para assegurar a liberdade de manobra[6].

O Exército, o Ciberespaço e as Operações de Estabilização

A atual doutrina trata inadequadamente dos imperativos cibernéticos para as operações de estabilização. E, como até mesmo os países mais pobres do mundo hoje dependem do ciberespaço — áreas onde, mais provavelmente, as operações militares norte-americanas serão conduzidas com parceiros da coalizão no futuro —, a doutrina militar dos EUA deve considerar formas pelas quais o ciberespaço influencia, simultaneamente, todas as linhas de esforço durante as operações de estabilização.

Os EUA preveem que suas Forças Armadas se adestrem e executem operações de estabilização independentemente do ambiente de informações incerto da atualidade. As operações de estabilização envolvem "várias missões, tarefas e atividades militares conduzidas fora dos EUA em coordenação com outros instrumentos do poder nacional, para manter ou restabelecer um ambiente seguro e prestar serviços governamentais essenciais, reconstrução emergencial de infraestrutura e ajuda humanitária"[7]. Notadamente, todas as operações conjuntas se apoiam no ciberespaço, o qual capacita a Força Conjunta a integrar operações nos domínios terrestre, aéreo, marítimo e espacial[8]. Em consequência, o Exército dos EUA também deve se adestrar para, potencialmente, obter a segurança cibernética essencial para um país anfitrião durante operações de estabilização.

Redes Móveis Sem Fio: Exemplos de um Serviço Essencial que Depende do Ciberespaço

Uma manifestação do ciberespaço são as redes móveis sem fio civis. Crises recentes comprovaram que essas redes móveis são indispensáveis para os socorristas. Por exemplo, durante o surto de Ebola, em 2014, o governo de Sierra Leone utilizou mensagens de texto para transmitir mensagens de saúde pública[9]. O compartilhamento móvel de dados também foi essencial nos esforços de recuperação após os terremotos de 2010 no Haiti e no Chile[10]. Além disso, após o terremoto de 2015 no Nepal, as redes móveis possibilitaram comunicações cruciais entre os agentes humanitários e os cidadãos locais. Com as linhas telefônicas sobrecarregadas, os sobreviventes nepaleses se apoiaram na internet para compartilhar informações[11].

As redes móveis se mostraram indispensáveis mais uma vez durante a resposta ao desastre provocado pelo terremoto e tsunami de 2011 no Japão, quando os cidadãos locais dependeram, fortemente, de redes móveis para acessar informações de emergência cruciais[12]. Essa dependência também foi exemplificada após as explosões de bombas na Maratona de Boston, em 2013, e o terremoto em São Francisco, em 2007, quando cidadãos ansiosos sobrecarregaram as redes móveis com um enorme aumento de tráfego[13].

Depois que o tufão Haiyan atingiu as Filipinas, em 2013, os habitantes e organizações de assistência tiveram dificuldades em recuperar o serviço móvel[14]. Durante as operações de socorro, a Comissária da União Europeia (UE) para a Cooperação Internacional, Ajuda Humanitária e Resposta a Crises, Kristalina Georgieva, afirmou: "A primeira [prioridade] é obter acesso a áreas remotas o mais rápido possível, e a questão de acesso se refere tanto ao transporte quanto ao restabelecimento das telecomunicações"[15].

Antes de o Tufão Haiyan tocar o solo, a entidade Groupe Speciale Mobile Association (GSMA) enviou uma equipe de resposta a desastres para ajudar o governo filipino e as companhias de telecomunicações do país a pré-posicionarem suas iniciativas de resposta[16]. A GSMA é um órgão da indústria que representa mais de 250 companhias de telecomunicações, como a AT&T, Orange, Telenor, Verizon e Vodafone[17]. Depois que o tufão tocou o solo, os representantes da GSMA ajudaram a restabelecer redes de compartilhamento de informações para possibilitar serviços essenciais como o "dinheiro móvel" (a utilização de dispositivos como telefones móveis para transferir quantias, em vez de se usar dinheiro vivo)[18].

A GSMA explica: "Os dispositivos móveis são, com frequência, uma das primeiras coisas às quais as pessoas recorrem no caso de um desastre; por exemplo, um dos primeiros pedidos dos habitantes deslocados na Montanha de Sinjar, no Iraque, foi um modo de carregar seus telefones móveis, para que pudessem obter informações, localizar entes queridos e participar de esforços de resposta"[19]. Esses exemplos ilustram que, em 2015, as redes móveis haviam se tornado, verdadeiramente, um componente essencial da gestão de crises.

Além das comunicações em si, os telefones móveis possibilitaram os serviços bancários móveis. Em janeiro de 2015, 38% da população mundial vivia sem acesso a uma conta bancária; os serviços bancários móveis prometem uma via principal de acesso para essas comunidades[20]. Por exemplo, a maior instituição financeira do Paquistão é uma operadora de telefonia móvel norueguesa[21]. Em um outro exemplo, o Quênia possui um dos sistemas de pagamento por telefone móvel mais populares e bem-sucedidos do mundo[22].

Contudo, em um relatório de 2011, a Equipe de Prontidão para Emergências Computacionais, do Departamento de Segurança Interna (*Department of Homeland Security — DHS*) dos EUA, advertiu que "os telefones móveis estão se tornando cada vez mais valiosos como alvos de ataque"[23]. Os profissionais de segurança cibernética consideram os dispositivos móveis como a maior vulnerabilidade de suas redes[24]. Entre agosto de 2013 e março de 2014, o número mensal de ataques contra dispositivos móveis aumentou em mais de 800%[25]. Em um caso, criminosos cibernéticos chineses utilizaram aplicativos falsos de serviços bancários móveis para induzir os usuários a inserirem seus dados, possibilitando que hackers roubassem milhões de dólares[26]. Considerando que as comunidades em futuros conflitos dependerão de serviços bancários móveis, as ameaças cibernéticas a tais serviços influenciarão as operações de estabilização do Exército.

Proteção e Restabelecimento de Serviços Essenciais que Dependem do Ciberespaço

A comunidade internacional desempenha um papel fundamental em ajudar as partes envolvidas a restabelecer as telecomunicações como um serviço essencial. A União Internacional de Telecomunicações (UIT) é a agência da Organização das Nações Unidas encarregada de supervisionar as tecnologias da informação e comunicação (TIC). A UIT inclui, entre seus integrantes, 173 governos e centenas de instituições não governamentais e empresas privadas[27]. No primeiro trimestre de 2015, foram enviados funcionários da UIT incumbidos de ajudar a restabelecer serviços de telecomunicações para ações de socorro em Maláui, Moçambique, Micronésia, Nepal e Vanuatu[28]. Os esforços na área de telecomunicações representam um imperativo mais amplo para o crescimento das TIC, visando à estabilidade.

(Foto do 2º Sgt Ryan Whitney, Com Soc, 1ª Ala de Op Esp)

Militares ucranianos monitoram e mantêm o acesso à rede durante o Exercício *Combined Endeavor* 2011, em Grafenwoehr, na Alemanha, 19 Set 11. Esse exercício anual, que envolve quase 40 parceiros da OTAN, Parceria para a Paz e segurança estratégica, destina-se a aumentar a interoperabilidade e a aperfeiçoar os processos de comunicação entre os países participantes.

O Paradoxo Cibernético e Exemplos de Ameaças Emergentes

A proteção e o restabelecimento das TIC são componentes necessários da prosperidade[29]. O futuro crescimento econômico dependerá da mobilidade e flexibilidade das redes de um país[30]. Em 2007, a UIT enfatizou: "As organizações e países precisam concentrar-se em capacidades de inovação e rápida adaptabilidade, apoiados por um sistema de informações poderoso e seguro, caso queiram sobreviver e impor-se como atores de longo prazo no novo ambiente competitivo"[31]. O maior acesso à internet, a serviços móveis e à banda larga estimula o crescimento econômico[32]. Além disso, o Banco Mundial identifica as TIC como fatores-chave no desenvolvimento social[33]. À medida que países em desenvolvimento continuarem a ampliar a penetração de suas TIC, seus custos de longo prazo com respeito à infraestrutura diminuirão, criando, assim, um círculo "virtuoso"[34]. Esses custos decrescentes ocasionam uma penetração ainda maior de banda larga[35]. Em suma, as TIC liberam forças econômicas latentes em economias em desenvolvimento[36].

Em um relatório de 2014, pesquisadores da Microsoft descreveram um "paradoxo de segurança cibernética" que se coloca diante de países em desenvolvimento com uma baixa penetração de TIC[37]. Esses países sofrem as taxas mais elevadas de infecção de *malware*. Além disso, à medida que desenvolvem a infraestrutura de TIC, suas taxas de infecção crescem[38]. Assim, os países mais pobres, com os menores níveis de TIC, podem ser extremamente vulneráveis a ameaças à segurança cibernética.

Considerando que as zonas de conflito já sofrem níveis elevados de tráfico de pessoas, exploração infantil, comércio de drogas ilícitas e crime organizado, um ciberespaço vulnerável as deixa prontas para serem exploradas[39]. Em consequência, o crime cibernético passou a ser uma evolução inevitável para elementos perigosos, nessas circunstâncias. Por exemplo, após o terremoto de 2010 no Haiti, criminosos cibernéticos

publicaram, imediatamente, portais de internet para entidades beneficentes falsas, a fim de explorar doadores[40].

Em outros lugares, os ataques cibernéticos passaram a ser um componente do conflito político. Por exemplo, quando a Rússia se apossou da Crimeia, em 2014, operadoras de telefonia móvel na Ucrânia sofreram significativas interrupções de serviço[41]. Além disso, durante a eleição presidencial de maio de 2014 na Ucrânia, *hackers* pró-Rússia penetraram o sistema de voto eletrônico e instalaram um código malicioso capaz de deletar uma grande quantidade de votos[42].

Em resposta, em fevereiro de 2015, Kiev publicou uma nova estratégia de segurança cibernética, que estabeleceu "um 'cadastro nacional de objetos cruciais da infraestrutura nacional de TI,' visando a assegurar sua proteção"[43]. Apesar desses esforços, um suposto ataque cibernético conduzido em 23 Dez 15 deixou mais de 700 mil ucranianos sem eletricidade[44]. A experiência da Ucrânia demonstra a relevância da segurança cibernética para as operações de estabilização.

Parcerias entre os Setores Público e Privado

Como Kiev, os EUA continuam a aprimorar a política relativa à segurança cibernética e à proteção de infraestrutura crítica, para se adaptarem a ameaças emergentes. A infraestrutura crítica, conforme definida na diretriz presidencial PPD-21 (*Presidential Policy Directive 21*), consiste nos "sistemas e meios, quer sejam físicos quer virtuais, tão vitais para os EUA que sua incapacidade ou destruição teria um efeito debilitante sobre a defesa, segurança econômica nacional, segurança ou saúde pública nacional ou qualquer combinação dessas questões"[45]. Os EUA classificam a infraestrutura crítica em dezesseis setores, que abarcam da energia ao transporte.

A discussão sobre a proteção de infraestrutura crítica e as consequentes implicações e mudanças com respeito a políticas ganharam destaque nos últimos 20 anos. Em 2002, o Departamento de Segurança Interna assumiu um papel central na proteção de infraestrutura crítica[46]. Até mesmo antes disso, o decreto EO 13010 (*Executive Order 13010*), expedido pelo Presidente Bill Clinton, em 1996, classificou as ameaças à infraestrutura crítica como físicas e cibernéticas[47]. Quase duas décadas depois, o documento *2014 Quadrennial Homeland Security Review* ("Revisão Quadrienal de Segurança Interna de 2014", em tradução livre) enfatizou os consideráveis efeitos destrutivos potenciais das ameaças cibernéticas à infraestrutura crítica[48].

Necessidade de Cooperação Governamental, Militar e Civil na Proteção do Ciberespaço

O aspecto central de uma efetiva segurança cibernética e proteção de infraestrutura crítica é a colaboração entre os setores público e privado. Em 2013, o decreto EO 13636, do Presidente Barack Obama, reforçou a

(Foto do 2º Sgt David Bruce, 38ª Div Inf)

Mais de 350 pessoas, incluindo militares da Guarda Nacional, militares da Força Aérea e civis, oriundos de 42 Estados, participaram do Exercício *Cyber Shield*, realizado em Camp Atterbury, Indiana, entre os dias 9 e 20 de março de 2015. O objetivo foi o de adestrar os participantes a defender a infraestrutura crítica contra ataques cibernéticos. O exercício incluiu uma competição em que 24 equipes combateram no ciberespaço para proteger os computadores e correspondentes sistemas de controle industriais de uma cidade simulada contra adversários maliciosos extremamente habilidosos. Uma equipe combinada do Oregon e de Idaho venceu a competição.

segurança cibernética para a proteção de infraestrutura crítica por meio da colaboração entre os setores público e privado, determinando que o Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology — NIST*) desenvolvesse "um modelo para reduzir riscos cibernéticos à infraestrutura crítica"[49]. Em 2014, o NIST divulgou uma versão preliminar, que ratificava a cooperação entre os setores público e privado na segurança cibernética[50].

Singer e Friedman ressaltam: "o setor privado controla cerca de 90% da infraestrutura crítica dos EUA, e as firmas por trás dela utilizam o ciberespaço para, entre outras coisas, equilibrar os níveis de cloração da água da sua cidade, controlar o fluxo de gás que aquece sua casa e executar as transações financeiras que mantêm a estabilidade cambial"[51]. O Subsecretário de Segurança Cibernética e Comunicações do Departamento de Segurança Interna, Andy Ozment, explica: "Não há a menor possibilidade de que o governo possa ajudar todas as empresas dos EUA a se protegerem"[52]. A cooperação entre os setores público e privado é fundamental para a criação de um modelo adaptável de segurança cibernética[53].

Em 1998, a diretriz presidencial PDD-63 (*Presidential Decision Directive 63*) estabeleceu Centros de Compartilhamento e Análise de Informações (*Information Sharing and Analysis Center — ISAC*), que convidam as partes envolvidas do segmento privado a desenvolverem redes para compartilhar melhores práticas e facilitar a resposta a crises[54]. Esses centros se apoiam na indústria privada no caso de "missões sem teor regulamentar ou de segurança pública"[55]. São "um órgão central de troca de informações entre e dentro dos vários setores, fornecendo uma biblioteca para dados históricos a serem utilizados pelo segmento privado e, conforme considerado apropriado pelo ISAC, pelo governo"[56]. Desde 1998, o modelo dos ISAC evoluiu para facilitar a cooperação entre os governos dos âmbitos federal, estadual, local, tribal e territorial.

Em 2013, a diretriz presidencial PPD-21 determinou que o Departamento de Segurança Interna criasse dois centros nacionais para supervisionar a proteção da infraestrutura física e cibernética[57]. O Departamento incorporou essa orientação em seu *Plano Nacional de Proteção da Infraestrutura*[58]. O Centro Nacional de Coordenação de Infraestrutura (*National Infrastructure Coordinating Center — NICC*) supervisiona o domínio físico e o Centro Nacional de Integração de Segurança Cibernética e Comunicações (*National Cybersecurity and Communications Integration Center — NCCIC*) lida com o domínio cibernético[59]. Esses centros de coordenação também facilitam a colaboração entre os setores público e privado por meio dos ISAC.

Em fevereiro de 2015, o decreto EO 13691 determinou que o Departamento de Segurança Interna dos EUA desenvolvesse Organizações de Compartilhamento e Análise de Informações (*Information Sharing and Analysis Organizations — ISAO*)[60]. Essas organizações estendem o modelo dos ISAC além dos 16 setores de infraestrutura crítica, de modo a incluir outros setores prioritários, como firmas de advocacia e contabilidade, que são alvos principais para ataques cibernéticos[61]. O decreto EO 13691 determina que o NCCIC supervisione os planos das ISAO[62]. As ISAO, ainda em seu início, buscam proporcionar a cooperação apesar da desconfiança e atrito entre o governo e outras partes envolvidas. Esse "jogo de malabarismo" se assemelha ao futuro ambiente de informações do Exército, afetando, significativamente, sua condução das operações de estabilização.

Conclusão

Segundo a doutrina, as operações de estabilização exigem coordenação com o governo do país anfitrião, indústria comercial, parceiros multinacionais e até mesmo organizações não governamentais. Essa mentalidade de cooperação se aplica às operações cibernéticas. Como os governos dependem do ciberespaço para fornecer serviços essenciais, a segurança cibernética requer uma sexta linha de esforço que apoie, simultaneamente, as outras cinco tarefas das operações de estabilização identificadas na Publicação Doutrinária do Exército dos EUA 3-07, *Estabilidade* (*ADP 3-07, Stability*)[63]:

- Estabelecer a segurança civil
- Estabelecer o controle civil
- Restabelecer serviços essenciais
- Apoiar a governança
- Apoiar o desenvolvimento econômico e de infraestrutura
- *Proteger a infraestrutura cibernética*

Na doutrina cibernética, o Estado-Maior Conjunto observa a importância de integrar os esforços cibernéticos com outras partes envolvidas. No documento

Cyber Strategy ("Estratégia Cibernética"), de 2015, o Departamento de Defesa dos EUA descreveu "Formar alianças, coalizões e parcerias no exterior" como uma atividade fundamental de segurança cibernética[64]. Em um memorando de junho de 2015, o Almirante Michael Rogers afirmou: "As operações cibernéticas demandam níveis inéditos de colaboração e compartilhamento de informações nos âmbitos conjunto, interagências e da coalizão; portanto, continuaremos a ser parceiros leais ao colaborarmos com outras agências, com aliados e amigos no exterior, com a indústria e com o meio acadêmico"[65]. O Estado-Maior Conjunto identificou sérios obstáculos à cooperação entre os setores público e privado em relação à segurança cibernética, alertando:

> Muitas organizações não governamentais hesitam em associar-se a organizações militares com qualquer tipo de relacionamento formal, especialmente no caso da condução de operações cibernéticas, porque isso poderia comprometer seu *status* como uma entidade independente, restringir sua liberdade de movimento e até colocar seus integrantes em perigo em ambientes permissivos incertos ou hostis[66].

Ao estabelecerem o modelo ISAC/ISAO, seus idealizadores buscaram superar tal desconfiança entre o governo, a indústria e as organizações não governamentais. Ainda que não constitua, de maneira alguma, uma panaceia, o modelo ISAC/ISAO oferece ao Exército dos EUA uma estrutura para facilitar a cooperação em futuras operações de estabilização.

Esse é um imperativo operacional tanto atual quanto futuro. Conforme o necessário, o Exército dos EUA deve estar pronto para restabelecer a segurança cibernética para a infraestrutura crítica em um país anfitrião por meio da coordenação de esforços com órgãos intergovernamentais, como a UIT; com a indústria privada, como os integrantes da GSMA; e com diversas organizações governamentais. Para facilitar a colaboração necessária, o modelo ISAC/ISAO fornece um ponto de partida para operações futuras.

O Major Michael Kolton, do Exército dos EUA, é aluno de pós-graduação no Jackson Institute for Global Affairs, da Yale University. Kolton é oficial especialista em assuntos sobre a China. Serviu, anteriormente, como oficial de Infantaria, em missões no Iraque e no Afeganistão. Possui os títulos de mestre em Economia pela University of Hawaii at Manoa e de bacharel em Economia pela Academia Militar dos EUA em West Point, Estado de Nova York.

Referências

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

2. Joint Publication (JP) 3-12(R) *Cyberspace Operations* (Washington, DC: U.S. Government Printing Office [GPO], 5 February 2013), p. 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* (Fort Eustis, VA: TRADOC, 31 October 2014), p. 11.

4. Joint Chiefs of Staff, *National Military Strategy of the United States 2015*, June 2015, 7, acesso em 11 dez. 2015, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

5. Ibid., p. 4 e p. 11.

6. JP 3-12(R), *Cyberspace Operations*, v; Gregory Conti, John Nelson and David Raymond, "Towards a Cyber Common Operating Picture" (presented at 5th International Conference on Cyber Conflict, Tallinn, Estonia, 4–7 June 2013), p. vi.

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

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

9. "Ebola in Sierra Leone: Which Doctor?" *Economist* (blog), 19 June 2014, acesso em 14 dez. 2015, http://www.economist.com/blogs/baobab/2014/06/ebola-sierra-leone.

10. "Online Crisis Management: A Web of Support", *Economist* (blog), 14 July 2011, acesso em 14 dez. 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 April 2015, acesso em 14 dez. 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* (blog), 24 April 2011, acesso em 14 dez.

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 April 2013, acesso em 14 dez. 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, November 2014, p. 20, acesso em 22 dez. 2015, http://www.cdacnetwork.org/contentAsset/raw-data/7825ae17-8f9b-4a05-bfbd-7eb9da6ea8c1/attachedFile.

15. "Typhoon Haiyan: Philippines Destruction 'Absolute Bedlam'" BBC News, 11 nov. 2013, acesso em 14 dez. 2015, http://www.bbc.com/news/world-asia-24894529.

16. Serena Brown, "The Private Sector: Stepping Up", *Humanitarian Exchange Magazine* 63 (January 2015), acesso em 1 jun. 2015, http://www.odihpn.org/humanitarian-exchange-magazine/issue-63/the-private-sector-stepping-up.

17. "Brief History of GSM & the GSMA", Groupe Speciale Mobile Association website, acesso em 22 dez. 2015, http://www.gsma.com/aboutus/.

18. "About the Mobile Money Programme", Groupe Speciale Mobile Association website, acesso em 23 December 2015, http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/about.

19. "GSMA Launches Humanitarian Connectivity Charter", Groupe Speciale Mobile Association Press Release, 2 March 2015, acesso em 22 dez. 2015, http://www.gsma.com/newsroom/press-release/gsma-launches-humanitarian-connectivity-charter/.

20. Asli Demirguc-Kunt et al., "The Global Findex Database 2014: Measuring Financial Inclusion around the World", World Bank Policy Research Working Paper 7255, April 2015, acesso em 14 dez. 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", IGATE Corporation White Paper, 2014, 2, acesso em 14 dez. 2015, http://www.igate.com/documents/11041/100349/Global_trends_in_Mobile_Banking.pdf/cf246d31-83c6-44b8-b6fb-a43f38ca2633.

22. Ibid.

23. Paul Ruggiero e Jon Foote, "Cyber Threats to Mobile Phones", report for U.S. Computer Emergency Readiness Team, prepared by Carnegie Mellon University, 2011, acesso em 22 dez. 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, p. 5, acesso em 22 dez. 2015, http://cyber-edge.com/wp-content/uploads/2014/01/CyberEdge--2014-CDR.pdf.

25. "Mobile Cyber Threats", Kaspersky Lab e INTERPOL Joint Report, October 2014, 13, acesso em 22 dez. 2015, http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyber-threats-web.pdf.

26. Pierluigi Paganini, "Yanbian Gang Steals Millions from Mobile Banking Customers of South Korea", *Security Affairs*, 18 February 2015, acesso em 22 dez. 2015, http://securityaffairs.co/wordpress/33709/cyber-crime/yanbian-gang-mobile-banking.html.

27. "ITU Disaster Response", ITU website, April 2015, acesso em 22 dez. 2015, http://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Response.aspx.

28. Ibid.

29. Alessandra Colecchia e 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*, July 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* (blog), 17 December 2013, acesso em 14 dez. 2015, http://www.economist.com/blogs/theworldin2014/2013/12/friends-and-forecasters.

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

32. Christine Zhen-Wei Qiang, "Mobile Telephony: A Transformational Tool for Growth and Development", *Private Sector Development* 4 (November 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, acesso em 22 dez. 2015, http://siteresources.worldbank.org/EXTIC4D/Resources/5870635-1242066347456/IC4D_2009_Chapter4.pdf.

34. Ibid.

35. "ICT Facts and Figures", International Telecommunication Union website, February 2013, acesso em 22 dez. 2015, https://www.itu.int/en/ITU-D//Statistics/Documents/facts/ICTFactsFigures-2013-e.pdf.

36. "The Role of Wi-Fi in Developing Nations", Wireless Broadband Alliance website, 24 April 2014, acesso em 22 dez. 2015, http://www.wballiance.com/industryinsights/the-role-of-wi-fi-in-developing-nations/.

37. David Burt et al., "The Cybersecurity Risk Paradox: Impact Social, Economic, and Technological Factors on Rates Malware", Microsoft Intelligence Report Special Edition, 2014, 2, acesso em 22 dez. 2015, http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity--Risk-Paradox.pdf.

38. Ibid., p. 8.

39. "Human Trafficking: A Brief Overview", *Social Development Notes Conflict, Crime and Violence* 122 (December 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 March 2011, acesso em 22 dez. 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 January 2010, acesso em 22 dez. 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 March 2014, acesso em 22 dez. 2015, http://foreignpolicy.com/2014/03/03/hack-attack/.

42. Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers", *Christian Science Monitor*, 17 June 2014, acesso em 25 fev. 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 February 2015, acesso em 22 dez. 2015, http://www.scmagazineuk.com/ukrainian-government-to-counter-cyber-attacks/article/397970/.

44. James Titcomb, "Ukrainian blackout blamed on cyber-attack", *Telegraph*, 5 January 2016, acesso em 6 jan. 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 February 2013, acesso em 22 dez. 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, and Larry Wentz, *Cyberpower and National Security* (National Defense University: Potomac Books, 1 April 2009), 132, Kindle edition; Richard White, "Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model", Homeland Security Affairs 10 (1) (February 2014): 2, acesso em 7 abr. 2015, https://www.hsaj.org/articles/254.

47. Executive Order 13010, "Critical Infrastructure Protection", 15 July 1996, acesso em 22 dez. 2015, http://fas.org/irp/offdocs/eo13010.htm.

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

49. "Foreign Policy: Cybersecurity", The White House website, acesso em 22 dez. 2015, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity; Executive Order 13636, "Improving Critical Infrastructure Cybersecurity", 12 February 2013, acesso em 22 dez. 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 February 2014, acesso em 22 dez. 2015, http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

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

52. Andy Ozment (Assistant Secretary for Cybersecurity and Communications DHS), "Cybersecurity and the Law", American Bar Association, 00:34:53, acesso em 22 dez. 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, February 2013), p. 8.

54. Kramer et al., *Cyberpower*, 131; Presidential Decision Directive (PDD-63), "Critical Infrastructure Protection", 22 May 1998, acesso em 22 dez. 2015, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

55. PDD-63, "Infrastructure Protection".

56. Ibid.

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, acesso em 22 dez. 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, acesso em 22 dez. 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 February 2015, acesso em 22 dez. 2015, http://www.gpo.gov/fdsys/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf.

61. "Information Sharing and Analysis Organizations", Homeland Security (18 March 2015), acesso em 10 abr. 2015, http://www.dhs.gov/isao.

62. "Information Sharing and Analysis Organizations Public Meeting", ISAO Transcripts (31 March 2015), acesso em 22 dez. 2015, http://www.dhs.gov/publication/isao-transcripts.

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

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

65. *Beyond the Build: Delivering Outcomes through Cyberspace* (Fort Meade, MD: US Cyber Command, 3 June 2015), p. 3.

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