(Photo by Khalil Senosi, Associated Press)

Amina Harun talks on a cell phone 26 July 2005 while selling watermelons at the largest fresh fruit and vegetable market in Nairobi, Kenya. Cell phone companies that set up shop in Africa over a decade ago now include poor farmers, fishermen, and the unemployed as subscribers. Some researchers even attach cell phones to elephants to help track their movements.

Host-Nation Cybersecurity in Future Stability Operations

Honorable Mention, 2015 DePuy Contest

Maj. Michael Kolton, U.S. Army

Cyberspace is now fundamental to the governance, economic growth, and social lives of populations within developed and developing countries. In addition, cyberspace capabilities have proven indispensable for relief efforts in disaster and conflict zones. Meanwhile, adversaries have also evolved in their sophistication and now increasingly threaten cyber capabilities.

Because nonmilitary organizations retain significant experience in cybersecurity and critical infrastructure protection, the best practices they have developed provide a framework for future Army doctrine. This article

explores integrating such precedents for host-nation cybersecurity during U.S. Army stability operations.

Defining Cyberspace

In defining cyberspace, security experts Peter Singer and Allan Friedman keep it simple: "At its essence, cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online."[1] Similarly, the U.S. military defines cyberspace as "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Over the next thirty years, the Army anticipates conflicts will grow more complex as adversaries leverage advanced technologies, including those that take the fight into the cyber domain.[3]

For America's homeland defense, the U.S. military has invested in cyber capabilities "to protect vital networks and infrastructure."[4] The Pentagon focuses cybersecurity efforts toward protecting military systems.[5] Current military cyberspace doctrine emphasizes securing the military's own information systems to ensure freedom of maneuver.[6]

The Army, Cyberspace, and Stability Operations

Current doctrine inadequately addresses the cyberspace imperatives for stability operations. And, since even the world's poorest countries are now reliant on cyberspace—the most likely areas in which U.S. military operations will be conducted with coalition partners in the future—U.S. military doctrine must consider ways in which cyberspace simultaneously influences all lines of effort during stability operations.

America expects its military to train for and execute stability operations regardless of today's uncertain information environment. Stability operations involve "various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief."[7] Notably, all joint operations rely on cyberspace, which enables the joint force to integrate operations across the land, air, maritime, and space domains.[8] Consequently, the Army must also train to potentially achieve essential cybersecurity for a host nation during stability operations.

Mobile Wireless Networks: Examples of an Essential Service Reliant on Cyberspace

One manifestation of cyberspace is civilian mobile wireless networks. Recent crises have proven that such mobile networks are indispensable for responders. For example, during the Ebola outbreak in 2014, the Sierra Leone government used text messages to transmit public health messages.[9] Mobile data sharing was also essential in recovery efforts after the 2010 earthquakes in Haiti and Chile.[10] And, after the 2015 earthquake in Nepal, mobile networks enabled lifesaving communication between relief workers and local citizens. With phone lines overwhelmed, Nepalese survivors relied on the Internet to share information.[11]

Mobile networks again proved indispensable during the response to the 2011 earthquake and tsunami disaster in Japan, when local citizens depended heavily on mobile networks to access critical emergency information.[12] This dependency was also exemplified after the 2013 Boston Marathon bombing and the 2007 San Francisco earthquake when anxious citizens overwhelmed mobile networks with a massive traffic surge.[13]

After Typhoon Haiyan struck the Philippines in 2013, residents and aid organizations struggled to regain mobile service.[14] During relief operations, European Union (EU) Commissioner for International Cooperation, Humanitarian Aid, and Crisis Response Kristalina Georgieva said, "The first [priority] is to get access to remote areas as quickly as possible, and the access issue is both transportation and also restoring telecommunications."[15]

Before Typhoon Haiyan made landfall, Groupe Speciale Mobile Association (GSMA) deployed a disaster response team to help the Filipino government and the country's telecommunications companies pre-position their response efforts.[16] GSMA is an industry body representing over 250 telecommunications companies like AT&T, Orange, Telenor, Verizon, and Vodafone.[17] After the typhoon struck, GSMA's representatives helped restore information-sharing networks to enable essential services such as mobile money (the use of devices such mobile phones to transfer money in lieu of cash).[18]

GSMA explains, "Mobile devices are often one of the first things people reach for when disaster strikes; for example, one of the first requests by those displaced on Sinjar Mountain in Iraq was a means to charge their mobile phones so that they could obtain information, to locate loved ones, and to become involved in response efforts."[19] Those examples illustrate that, by 2015, mobile networks had truly become an essential component of crisis management.

Beyond straightforward communications, mobile phones have also enabled mobile banking. As of January 2015, 38 percent of the world's population lived without access to a bank account; mobile banking promises the primary pathway for such communities.[20] For example, Pakistan's largest financial institution is a Norwegian mobile phone operator.[21] In another example, Kenya boasts one of the most popular and successful mobile phone payment systems in the world.[22]

However, in a 2011 report, the Department of Homeland Security's (DHS) Computer Emergency Readiness Team warned "mobile phones are becoming more and more valuable as targets for attack."[23] Cybersecurity professionals consider mobile devices their networks' greatest vulnerability.[24] Between August 2013 and March 2014, attacks per month against mobile devices increased over 800 percent.[25] In one instance, Chinese cybercriminals used fake mobile banking apps to trick users to enter credentials, which enabled hackers to steal millions of dollars.[26] Since communities in future conflicts will be dependent on mobile banking, cyberthreats to mobile banking will influence Army stability operations.

Protecting and Restoring Essential Services Reliant on Cyberspace

The international community plays a critical role in helping stakeholders restore telecommunications as an essential service. The International Telecommunication Union (ITU) has a United Nations mandate to oversee information and communications technologies (ICTs). ITU members include 173 governments and hundreds of nongovernmental institutions and private companies.[27] In the first quarter of 2015, ITU personnel deployed to help restore telecommunications for relief efforts in Malawi, Mozambique, Micronesia, Nepal, and Vanuatu.[28] Efforts in telecommunications represent a broader imperative for ICT growth for stability.

The Cyberspace Paradox and Examples of Emerging Threats

Protecting and restoring ICTs are necessary components of prosperity.[29] Future economic growth will depend upon the mobility and flexibility of a country's networks.[30] In 2007, ITU emphasized, "Organizations and countries need to focus on innovation capacities and rapid adaptability, backed up by a powerful and secure information system, if they wish to survive and assert themselves as long-term players in the new competitive environment."[31] Increased access to the Internet, mobile services, and broadband boosts economic growth.[32] Moreover, the World Bank identifies ICTs as key factors in social development.[33] As developing countries continued to deepen their ICT penetration, their long-run infrastructure costs decrease, thus creating a virtuous cycle.[34] Those falling costs spur even more broadband penetration.[35] In short, ICTs unleash latent economic forces in developing economies.[36]

In a 2014 report, Microsoft researchers described a "cybersecurity paradox" facing developing countries with low ICT penetration.[37] Those countries suffer the highest malware infection rates. Moreover, as those countries develop ICT infrastructure, their infection rates accelerate.[38] Thus, the poorest countries with the lowest ICT levels can be most vulnerable to cybersecurity threats.

Since conflict zones already suffer elevated levels of human trafficking, child exploitation, illicit drug trade, and organized crime, vulnerable cyberspace makes them ripe for exploitation.[39] Consequently, cybercrime has become an unavoidable evolution for nefarious actors in such circumstances. For example, after the 2010 Haiti earthquake, cybercriminals immediately published web portals for fake charities to bilk donors.[40]

Elsewhere, cyberattacks have become a component in political conflict. For example, when Russia seized the Crimea in 2014, mobile phone operators in Ukraine suffered significant service disruption.[41] And, during Ukraine's May 2014 presidential election, pro-Russian hackers penetrated the electronic voting system and installed malicious code capable of deleting swaths of votes.[42]

In response, in February 2015, Kiev published a new cybersecurity strategy that establishes "a 'national registry of crucial objects of national IT infrastructure,' with the aim ensuring their protection."[43] Notwithstanding these efforts, an alleged cyberattack on 23 December 2015

(Photo by Staff Sgt. Ryan Whitney, 1st Special Operations Wing Public Affairs)

Members of the Ukraine military monitor and maintain network access during Combined Endeavor 2011 in Grafenwoehr, Germany, 19 September 2011. Combined Endeavor, an annual exercise involving nearly forty NATO, Partnership for Peace, and strategic security partners, is designed to increase interoperability and enhance communications processes between the participating nations.

left over seven hundred thousand Ukrainians without electricity.[44] Ukraine's experience demonstrates cybersecurity's relevance to stability operations.

Public-Private Partnerships

Like Kiev, the United States continues to refine policy for cybersecurity and critical-infrastructure protection (CIP) to adapt to emerging threats. Critical infrastructure, as defined in Presidential Policy Directive 21, are "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[45] The United States categorizes critical infrastructure into sixteen sectors from energy to transportation.

Discussion of CIP, as well as the resulting policy implications and changes, has come to the forefront in the last twenty years. In 2002, DHS assumed a lead role in CIP.[46] Even before that, President Bill Clinton's 1996 Executive Order (EO) 13010 categorized critical infrastructure threats as physical and cyber.[47] Nearly two decades later, the *2014 Quadrennial Homeland Security Review* emphasized the significant potential destructive effects of cyberthreats to critical infrastructure.[48]

Need for Government, Military, and Civilian Cooperation in Protection of Cyberspace

The centerpiece of effective cybersecurity and CIP is public-private collaboration. In 2013, President Barack Obama's EO 13636 enhanced cybersecurity for CIP through public-private collaboration and directed the National Institute of Standards and Technology (NIST) to develop "a framework to reduce cyber risks to critical infrastructure."[49] In 2014, NIST released a preliminary framework affirming public-private cooperation in cybersecurity.[50]

Singer and Friedman point out, "the private sector controls roughly 90 percent of U.S. critical infrastructure, and the firms behind it use cyberspace to, among other things, balance the levels chlorination in your city's water, control the flow of gas that heats your home, and execute the financial transactions that keep currency prices stable."[51] DHS Assistant Secretary for Cybersecurity and Communications Andy Ozment explains, "There's no way that the government is going to be able to help every company in America secure itself."[52] Public-private cooperation is fundamental to building an adaptive cybersecurity framework.[53]

In 1998, Presidential Decision Directive 63 launched Information Sharing and Analysis Centers (ISACs), which invite private sector stakeholders to build networks to exchange best practices and facilitate crisis response.[54] ISACs rely on private industry for "non-regulatory and non-law enforcement missions."[55] They are "a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government."[56] Since 1998, the ISACs model has evolved to facilitate cooperation between federal, state, local, tribal, and territorial governments.

In 2013, PPD-21 ordered DHS to create two national centers to oversee physical and cyber infrastructure protection.[57] DHS incorporated this guidance in its *National Infrastructure Protection Plan*.[58] The National Infrastructure Coordinating Center oversees the physical domain, and the National Cybersecurity and Communications Integration Center (NCCIC) handles the cyber domain.[59] These coordination centers also facilitate public-private collaboration through the ISACs.

In February 2015, EO 13691 directed DHS to develop Information Sharing and Analysis Organizations (ISAOs).[60] These organizations extend the ISACs model beyond the sixteen critical infrastructure sectors to other high-value sectors like law and accounting firms, which are prime targets for cyberattacks.[61] EO 13691 directs the NCCIC to supervise ISAO arrangements.[62] Still in its infancy, ISAOs seek to provide cooperation despite distrust and friction between the government and other stakeholders. Such a balancing act parallels the Army's future information environment and significantly impacts the Army's conduct of stability operations.

Conclusion

Stability operations doctrinally require coordination with the host-nation government, commercial industry, multinational partners, and even nongovernmental organizations (NGOs). This cooperative mindset applies to cyberspace operations. Since governments rely on cyberspace to provide essential services, cybersecurity requires a sixth line of effort that simultaneously supports the

(Photo by Staff Sgt. David Bruce, 38th Infantry Division)

More than 350 National Guard soldiers, airmen, and civilians from forty-two states converged 9–20 March 2015 at Camp Atterbury, Indiana, to participate in Cyber Shield. The intent was to train the participants to defend critical infrastructure against cyberattacks. The exercise included a competition in which twenty-four teams battled in cyberspace to protect a mock city's computers and related industrial control systems against malicious, highly skilled adversaries. A combined team from Oregon and Idaho won the competition.

other five tasks for stability operations identified in Army Doctrine Publication 3-07, *Stability*:[63]

- Establish civil security
- Establish civil control
- Restore essential services
- Support to governance
- Support to economic and infrastructure development
- *Secure cyberspace infrastructure*

In cyberspace doctrine, the Joint Staff notes the importance of integrating cyber efforts with other stakeholders. In its 2015 *Cyber Strategy*, the Department of Defense described "Building alliances, coalitions, and partnerships abroad" as a fundamental cybersecurity activity.[64] In a June 2015 memorandum, Adm. Michael Rogers writes, "Cyberspace operations demand unprecedented degrees of joint, interagency, and coalition collaboration and information sharing, and thus we will remain trusted partners in collaborating with other agencies, with allies and friends abroad, with industry, and with academia."[65] The Joint Staff has identified profound obstacles to public-private cooperation on cybersecurity warning,

> Many NGOs are hesitant to become associated with military organizations in any form of formal relationship, especially in the case of conducting CO [cyberspace operations], because doing so could compromise their status as an independent entity, restrict their freedom of movement, and even place their members at risk in uncertain or hostile permissive environments.[66]

In building the ISAC/ISAO model, its architects have sought to surmount such distrust among government, industry, and NGOs. Though by no means a panacea, the ISAC/ISAO model offers the Army a framework for facilitating cooperation in future stability operations.

This is both a current and a future operational imperative. As required, the Army must be ready to restore cybersecurity for the critical infrastructure in a host nation by coordinating efforts with intergovernmental organizations like ITU, private industry like GSMA members, and various governmental organizations. To facilitate necessary collaboration, the ISAC/ISAO model provides a starting point for future operations.

Maj. Michael Kolton, U.S. Army, is a graduate student at Yale University's Jackson Institute for Global Affairs. Kolton is a foreign area officer specializing in China. He previously served as an infantry officer with deployments to Iraq and Afghanistan. He holds an MA in economics from the University of Hawaii at Manoa and a BA in economics from the United States Military Academy at West Point, New York.

Notes

1. Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (London: Oxford University Press, 2014), 13.
2. Joint Publication (JP) 3-12(R) *Cyberspace Operations* (Washington, DC: U.S. Government Printing Office [GPO], 5 February 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* (Fort Eustis, VA: TRADOC, 31 October 2014), 11.
4. Joint Chiefs of Staff, *National Military Strategy of the United States 2015*, June 2015, 7, accessed 11 December 2015, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
5. Ibid., 4 and 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), vi.
7. JP 3-07, *Stability Operations* (Washington, DC: U.S. GPO, 29 September 2011), vii.
8. JP 3-12 (R), *Cyberspace Operations*.
9. "Ebola in Sierra Leone: Which Doctor?" *Economist* (blog), 19 June 2014, accessed 14 December 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, accessed 14 December 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, accessed 14 December 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, accessed 14 December 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, accessed 14 December 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, 20, accessed 22 December 2015, http://www.cdacnetwork.org/contentAsset/raw-data/7825ae17-8f9b-4a05-bfbd-7eb9da6ea8c1/attachedFile.

15. "Typhoon Haiyan: Philippines destruction 'absolute bedlam,'" BBC News, 11 November 2013, accessed 14 December 2015, http://www.bbc.com/news/world-asia-24894529.

16. Serena Brown, "The Private Sector: Stepping Up," Humanitarian Exchange Magazine 63 (January 2015), accessed 1 June 2015, http://odihpn.org/wp-content/uploads/2015/01/HE_63_new_web2.pdf.

17. "About Us," Groupe Speciale Mobile Association website, accessed 22 December 2015, http://www.gsma.com/aboutus/.

18. "The Mobile Money ecosystem opportunity," Groupe Speciale Mobile Association website, accessed 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, accessed 22 December 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 (English)," World Bank Policy Research Working Paper 7255, April 2015, accessed 14 December 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, accessed 14 December 2015, http://www.igate.com/documents/11041/100349/Global_trends_in_Mobile_Banking.pdf/cf246d31-83c6-44b8-b6fb-a43f38ca2633.

22. Ibid.

23. Paul Ruggiero and Jon Foote, "Cyber Threats to Mobile Phones," report for U.S. Computer Emergency Readiness Team, prepared by Carnegie Mellon University, 2011, accessed 22 December 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, accessed 22 December 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, accessed 22 December 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 February 2015, accessed 22 December 2015, http://securityaffairs.co/wordpress/33709/cyber-crime/yanbian-gang-mobile-banking.html.

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

28. Ibid.

29. Alessandra Colecchia and 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, 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, accessed 14 December 2015, http://www.economist.com/blogs/theworldin2014/2013/12/friends-and-forecasters.

31. *Cybersecurity Guide for Developing Countries* (Geneva: Telecommunication Development Bureau, 2007), 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), 4, accessed 22 December 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, accessed 22 December 2015, https://www.itu.int/en/ITU-D//Statistics/Documents/facts/ICTFacts-Figures2013-e.pdf.

36. "The role of Wi-Fi in developing nations," Wireless Broadband Alliance website, 24 April 2014, accessed 22 December 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, accessed 22 December 2015, http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity-Risk-Paradox.pdf.

38. Ibid., 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, accessed 22 December 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, accessed 22 December 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, accessed 22 December 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, accessed 25 February 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, accessed 22 December 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, accessed 6 January 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, accessed 22 December 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, accessed 7 April 2015, https://www.hsaj.org/articles/254.

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

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

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

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

52. Andy Ozment (Assistant Secretary for Cybersecurity and Communications DHS), "Cybersecurity and the Law," American Bar Association, 00:34:53, accessed 22 December 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), 8.

54. Kramer et al., *Cyberpower,* 131; Presidential Decision Directive (PDD-63), "Critical Infrastructure Protection," 22 May 1998, accessed 22 December 2015, https://www.gpo.gov/fdsys/pkg/FR-1998-08-05/pdf/98-20865.pdf.

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, accessed 22 December 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, accessed 22 December 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, accessed 22 December 2015, http://www.gpo.gov/fdsys/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf.

61. "Information Sharing and Analysis Organizations," Homeland Security, 14 December 2015, accessed 10 April 2015, http://www.dhs.gov/isao.

62. "Information Sharing and Analysis Organizations Public Meeting," ISAO Transcripts, 31 March 2015, accessed 22 December 2015, http://www.dhs.gov/publication/isao-transcripts.

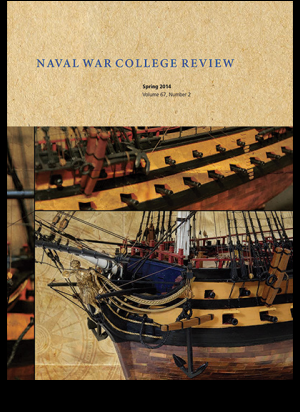
63. Army Doctrinal Publication 3-07, *Stability Operations* (Washington, DC: U.S. GPO, August 2012), 11.

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), 3.

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

MR We Recommend




CYBER WAR, CYBERED CONFLICT, AND THE MARITIME DOMAIN

Peter Dombrowski and Chris C. Demchak

If you found the above article enlightening, you may also like "Cyber War, Cybered Conflict, and the Maritime Domain" by Peter Dombrowski and Chris C. Demchak in the Spring 2014 edition of *Naval War College Review,* Volume 67, Number 2, online at https://www.usnwc.edu/Publications/Naval-War-College-Review/2014---Spring.aspx.