Perspectives on Cyber Power

CPP-3

The Achievable Multinational Cyber Treaty

Strengthening Our Nation's Critical Infrastructure

Mark A. Barrera
Colonel, USAF

Air Force Research Institute Papers

Air University

Steven L. Kwast, Lieutenant General, Commander and President

Air Force Research Institute

Dale L. Hayden, PhD, Director

AIR UNIVERSITY

Air Force Research Institute
Perspectives on Cyber Power

The Achievable Multinational Cyber Treaty

Strengthening Our Nation's Critical Infrastructure

Mark A. Barrera
Colonel, USAF

CPP–3

Air University Press
Air Force Research Institute
Maxwell Air Force Base, Alabama

Project Editor
James S. Howard

Copy Editor
Carolyn Burns

Cover Art, Book Design, and Illustrations
Daniel Armstrong

Composition and Prepress Production
Vivian D. O'Neal

Print Preparation and Distribution
Diane Clark

AIR FORCE RESEARCH INSTITUTE

AIR UNIVERSITY PRESS

Director and Publisher
Dale L. Hayden, PhD

Editor in Chief
Oreste M. Johnson

Managing Editor
Dr. Ernest Allan Rockwell

Design and Production Manager
Cheryl King

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
afri.aupress@us.af.mil

http://aupress.au.af.mil
http://afri.au.af.mil

Facebook:

https://www.facebook.com/AirUnivPress

and

Twitter: https://twitter.com/aupress

Library of Congress Cataloging-in-Publication Data

Names: Barrera, Mark A., 1970- author. | Air University (U.S.). Air Force Research Institute, issuing body.
Title: The achievable multinational cyber treaty : strengthening our nation's critical infrastructure / Mark A. Barrera.
Other titles: Strengthening our nation's critical infrastructure | Air Force Research Institute perspectives on cyber power ; CPP-3. 2329-5821
Description: First edition. | Maxwell Air Force Base, Alabama : Air University Press, Air Force Research Institute, 2016. | Series: Perspectives on cyber power, ISSN 2329-5821 ; CPP-3 | Includes bibliographical references.
Identifiers: LCCN 2016043993| ISBN 9781585662661 | ISBN 1585662666
Subjects: LCSH: Cyberterrorism—Prevention—International cooperation. | Cyber intelligence (Computer security)—International cooperation. | Cyberspace—Government policy—United States. | Cyberspace—International cooperation. | Computer crimes—International cooperation. | Cyberspace—Military aspects—United States. | Security, International. | United States. Strategic Command (2002-). Cyber Command. | Information warfare—United States—Prevention.
Classification: LCC HV6773.15.C97 B38 2016 | DDC 363.325—dc23 | SUDOC D 301.26/31:3

LC record available at https://lccn.loc.gov/2016043993

Published by Air University Press in February 2017

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air Force Research Institute, Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Air Force Research Institute Perspectives on Cyber Power

We live in a world where global efforts to provide access to cyber resources and the battles for control of cyberspace are intensifying. In this series, leading international experts explore key topics on cyber disputes and collaboration. Written by practitioners and renowned scholars who are leaders in their fields, the publications provide original and accessible overviews of subjects about cyber power, conflict, and cooperation.

As a venue for dialogue and study about cyber power and its relationship to national security, military operations, economic policy, and other strategic issues, this series aims to provide essential reading for senior military leaders, professional military education students, and interagency, academic, and private-sector partners. These intellectually rigorous studies draw on a range of contemporary examples and contextualize their subjects within the broader defense and diplomacy landscapes.

These and other Air Force Research Institute studies are available via the AU Press website at http://aupress.au.af.mil/papers.asp. Please submit comments to afri.public@maxwell.af.mil.

Contents

About the Author

Col Mark Barrera is assigned to the Air War College, Air University, Maxwell AFB, Alabama. Colonel Barrera entered the Air Force in 1993 after graduating from the Baylor University Reserve Officer Training Corps in 1992 and has served in various assignments in Air Force Materiel Command, Air Education and Training Command, Air Combat Command, Pacific Air Forces, US Air Forces in Europe, NATO, and US Air Forces Central Command. Colonel Barrera served as the commander of the 866th Air Expeditionary Squadron during Operation Enduring Freedom; chief of safety for Osan Air Base, Korea; division chief for the A-10C, F-22, and F-15E operational test programs; and chief of wing inspections, check flight commander, and financial/program manager for the Air Armament Center, Eglin AFB, Florida. He is a senior pilot with over 1,700 flying hours in the A-10 as a pilot and in the T-38 as an instructor and flight examiner. Before his selection for Air War College, Colonel Barrera was the chief of offensive plans and the US senior national representative at NATO Combined Air Operations Center Uedem at Uedem, Germany.

Abstract

The 2010 US *National Security Strategy* identifies large-scale cyber attacks to the nation's critical infrastructure as a major hazard to the homeland and announces the intention to reduce that vulnerability by pursuing diplomacy and supporting international norms of cyber behavior. Developing cyber norms and institutions is problematic, however. Competing interests exist among major state actors in the multinational environment—in particular Russia, China, and the United States—concerning information freedom and access. This paper will explain the genesis of these disagreements, propose that the United States move beyond the information-freedom debate, and then focus efforts on critical infrastructure security to further international cooperation. A survey of diplomatic, academic, and political literature indicates broad, global support for the protection of critical infrastructure, despite the limited progress in international agreements to date. Furthermore, analysis of the literature yields additional conclusions based on the reported efforts of the political and business actors regarding the critical infrastructure industry. Significant literature and public statements promote domestic actions to improve critical infrastructure security, but a lack of accountability limits the funding and the establishment of standards required to meet the objectives of the *National Security Strategy.* The United States has made incremental improvements in the legal and regulatory aspects of cybersecurity. However, additional federal regulatory powers could improve critical infrastructure protection. An international agreement covering critical infrastructure could also positively address the growing threats to our nation's networks.

The Problem

In 2012 former Secretary of Defense Leon Panetta warned the United States of a potential "cyber Pearl Harbor" attack on our nation's infrastructure, and the reality of the threat has already been demonstrated.[1] In December 2014 Germany's Federal Office for Information Security acknowledged that hackers breached an unnamed German industrial plant's control systems, preventing the shutdown of a furnace and thereby causing "widespread damage."[2] The 2010 US *National Security Strategy* (*NSS*) identifies large-scale cyber attacks on critical infrastructure as a major hazard to the homeland in the same context as terrorism, natural disasters, and pandemics. The *NSS* also calls for reducing these vulnerabilities through diplomacy and support for international norms of acceptable cyber behavior and cyber institutions to forestall the use of force in retaliation.[3] However, developing cyber norms and institutions has been problematic because of competing interests in the multinational environment. These difficulties center on the larger issue of information freedom and diminish chances for a multinational cyber treaty.[4]

Russia, China, and the United States have clashing ideologies concerning information freedom. The United States steadfastly supports the concept of freedom of information for the Internet, while Russia and China have resolutely proposed treaties at the United Nations emphasizing national sovereignty and state control of networks and information.[5] Despite this difference, several notable achievements have been made with international confidence-building measures, norms, and treaties. If the debate over information freedom and sovereignty could be resolved, critical-infrastructure security stands out as an area of possible international consensus and cooperation.

Examining the motives and actions of political and business actors involved within the critical-infrastructure industry might suggest additional measures needed to improve US national security. Focusing on these measures, together with efforts towards an international critical-infrastructure security agreement and improvements in national critical-infrastructure regulation and law, could positively address the growing threats to our nation's security.

A Clash of Ideologies in Cyberspace—Freedom versus State Control of Information

The *NSS* aims to "ensure the protection of the free flow of information and continued access," but it also identifies cyberspace as vulnerable to disruption and attack, representing "one of the most serious national security, public safety, and economic challenges we face as a nation."[6] The *NSS* elaborates on the need to protect critical infrastructure, calling the digital infrastructure a strategic national asset.[7] This emphasis on critical infrastructure builds on past policies, including Pres. Bill Clinton's 1998 *Presidential Decision Directive 63* and previously included in Pres. George W. Bush's *2003 National Strategy to Secure Cyberspace*.[8] The Department of Homeland Security (DHS) updated the *National Infrastructure Plan* in 2009 and the Department of Defense issued the *DOD Strategy for Operating in Cyberspace* in 2011to address critical-infrastructure cybersecurity.[9] President Barack Obama also signed an Executive Order in 2013 to support the nation's critical infrastructure owners and operators.[10]

The 2011 *International Strategy for Cyberspace* (*ISC*) reinforces the *NSS* regarding the dependence on the critical life-sustaining infrastructure and encourages all nations to strengthen international safeguards accordingly. The *ISC* calls for a consensus among like-minded states and "diplomacy, defense, and development" to promulgate norms of acceptable cyber behavior. The strategy also reaffirmed US aims to promote the fundamental freedom of expression, "respect for property, valuing privacy, protection from crime," and the right of self-defense. It further elaborates that states should not be persuaded to pursue security policies of "national-level" filters and firewalls but continue to support the growth of the Internet as an "open, interoperable, secure, and reliable medium of exchange."[11]

Russia, China, and Information Control

Russia, China, Tajikistan, and Uzbekistan proposed to the United Nations the *International Code of Conduct* (*ICC*) on 14 September, 2011.[12] Russia has been proposing draft resolutions on information security to the UN General Assembly every year since 1998 and pushed for a UN Group of Governmental Experts (GGE) report in 2003 to determine possible areas of cooperation to reduce political and military risk.[13] Despite no support for a 2003 GGE report, a GGE report was produced in 2010 recommending the international community develop and discuss norms and confidence-building measures.[14]

The *ICC* represents a push for sovereign control of information flows within a nation's borders to ensure national security and regime stability. Some have said Russia and China proposed the *ICC* to "regain the initiative" in internet governance and to gain international support.[15] Regardless, the *ICC* remains the fulcrum of debate over international cyber norms between the United States and Western nations that favor openness and human rights and the Eastern nations, Russia and China, which prefer to restrict Internet content to control their populations.

Russia's motives come from a doctrine that freedom of information and freedom of thought are threats to the state and that mass media control is essential in shaping the perceptions of their people and adversaries as well.[16] Examples include Russia's belief that the internal protests after its parliamentary elections in December 2011 were inspired and facilitated abroad by information spread on the Internet. Russia failed to ratify the Council of Europe's cybercrime treaty for reasons that included its resistance to data searches and discovery within its national networks.[17]

China has similar views concerning information security. The Chinese greatly fear internal threats from "uncontrolled mass access to information" and implement strong network supervision to maintain "social harmony."[18] China fiercely defends its national networks, contends that nations should respect the differing national perspectives about Internet security, and insists its military cyber operations are a response to the United States' "militarization of the Internet."[19] China also rejected the Council of Europe's cybercrime treaty for the same reasons as Russia. China will not allow foreign interference in its national networks.[20]

The United States disagrees with the *ICC,* defending civil liberties and the free flow of information.[21] The current method internet governance relies on international multistakeholder nongovernmental-organizations. The United States does not agree with the idea of replacing it with a regime based on a multilateral forum, such as the United Nations, essentially to protect state sovereignty.[22] The Department of State has also committed to "expose attempts to regulate Internet governance and increase control of cyberspace, particularly content in the name of social control."[23] Finally, some believe that the United States has rejected the *ICC* due to concerns that it would be impossible to enforce, and the United States clearly fears any concessions to support censorship and repressive domestic policies.[24]

The *ICC* represents the stalemate faced by the United States in its efforts to develop international agreements in cyberspace. It is a classic East–West debate over freedom versus control. However, the *ICC* expresses its consistent intention to "maintain the integrity of the infrastructure within States," and "protect the Internet and other information and communication technology networks from threats and vulnerabilities."[25] Also, the *ICC* asserts that states will not "use information and communications technologies, including networks, to carry out hostile activities" and urges all nations to "lead all elements of society, including its information and communication partnerships . . . in order to facilitate . . . the protection of critical information infrastructures."[26]

The development of international agreements has also been difficult due to lack of agreement on cybersecurity definitions, scope, and interests in the international community, in particular between the United States, Russia, and China.[27] However, there are areas of success including the Council of Europe's *Convention on Cybercrime,*[28] the UN Group of Government Experts reports, and the Organization for Security and Cooperation in Europe (OSCE) confidence-building measures (OCBM).

For context, the United States has become negatively identified as only interested in cyber agreements with primarily Western nations.[29] The United States is now perceived to be the leader in cyber military development and a source of several cyber attacks and exploitations.[30] Our cyber military leaders have openly expressed intentions to "dominate" cyberspace and have created the US Cyber Command.[31] This rhetoric may have been unhelpful within the world community, but the United States has increased its efforts to achieve international cyberspace agreements in recent years.

The United Nations has been working to develop a path for establishing international norms of behavior in cyberspace with some successes.[32] In 2010 the United States joined with several other nations in agreeing to consider confidence-building measures that address cyber conflict recommended by a GGE report.[33] This GGE report process did not develop quickly. As has been noted, Russia first proposed the creation of the GGE in 2003 to develop cooperation for the reduction of "political and military risk in the new digital environment."[34] The report of 2010 did slightly encourage the development of international norms of behavior and confidence-building measures. A 2013 GGE report produced an agreement between the major NATO allies, Russia, India, and the United States affirming that "international laws governing armed conflict apply to cyberspace," and that "existing internal commitments apply equally in cyberspace as they do in the physical domain."[35] This agreement is an enormously significant accomplishment, especially considering the United States' consistent support for the laws of armed conflict, which is consonant in US military doctrines. The United States complied with the OCBMs with the release of Joint Publication 3-12 *Cyber Operations* and stated US Air Force doctrine on cyber.[36]

The OCBMs are also significant achievements in the development of international agreements, particularly those regarding the use of information communication technologies (ICT) consistent with international law. The OCBMs specifically address the risk of misperceptions and the possible emergence of political or military tensions. In OCBMs, participating nations voluntarily share information regarding strategies, policies, and programs regarding the security and use of ICTs.[37] Russia participates (though China does not) in the OSCE and signed the measures with interpretive statements that address their sovereign information security guidelines.[38] As of November 2014, half of the 30 signing nations have either wholly or partially complied with the OCBMs.[39]

Synthesis—Freedom of Information Argument

The concept of freedom of information is considered a core principle in the United States' strategy for cyberspace, and it is promoted by the Department of State in the world community.[40] This concept seems to have broad support, notably by the 2014 NETmundial conference that advocated the freedom of expression and information.[41] The OSCE confidence-building measures promote an "open, interoperable, secure, and reliable Internet,"[42] which is word-for-word consistent with the US International Strategy for Cyberspace.[43] Nevertheless, Russia and China consistently disagree with the concept of freedom of information in state policies; they "consistently advocate the extension of state sovereign control and noninterference in cyberspace" and intend to "create national barriers" to carry out their policies.[44]

The United States should deemphasize the concept of information freedom in developing an international cyber treaty. The debate over sovereign control versus freedom of information in cyberspace appears to be insoluble; US interests may have already won, anyway. The United States should continue to champion the Universal Declaration of Human Rights (UDHR). The UN International Bill of Human Rights, which contains the UDHR, affirms, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers."[45] This treaty was ratified by Russia in 1973 and by China in 1998. The UN Special Rapporteur further clarified the meaning of the UDHR in 2011 to assure the world community that it applies to the Internet.[46] Some consider the *ICC* and its yearly proposals to the UN are merely devices to regain sovereignty lost by the ratification of the UDHR.[47] Freedom of expression and access to information should be defended, but more possible cyber agreements in the world community might be gained by focusing where there are broad consensuses regarding threats to critical infrastructure. Realization of those threats is more likely to cause harm to civilians and increase the possibility of international violence.

Critical Infrastructure Protection Treaty Debate

There is already broad support in the international community to establish measures or norms to protect national critical infrastructure and their connected industrial control systems (ICS). The European Network and Information Security Agency (ENISA) describes industrial control systems as command-and-control networks designed to support industrial processes. The largest subgroup of ICS is supervisory control and data acquisition (SCADA). Most of the ICS worldwide are legacy, proprietary, computer systems originally designed for operations unconnected to networks. However, now it is common for these control systems to be interconnected to increase efficiency and allow remote command and control. This interconnectivity allows hackers to gain access to ICS and cause serious damage.[48] What is most disturbing in this situation is that many control systems were designed and built long before there were any security concerns.[49]

The DHS is charged with assisting critical-infrastructure owners and operators. Critical infrastructures include agriculture, food, water, public health, emergency services, government, the defense industrial base, information and telecommunication, energy, transportation, banking and finance, the chemical industry, the postal system, and shipping.[50] Eighty-five percent of the nation's critical infrastructure is owned or operated by the private sector.[51] The cyberspace threats of technological and physical damage to critical infrastructures are real, and they dominate the headlines today with dramatic and potentially doomsday accounts. For example, a SCADA software bug in the northeastern United States caused an alarm system to fail after the disruption of a high-voltage power line. The software bug ultimately resulted in the deaths of 11 persons and $6 billion in damage from rail, air, energy, and communication shutdowns.[52] In another example from Australia, a disgruntled employee intentionally altered a computerized treatment plant's software to release 200,000 gallons of sewage into parks around a hotel, resulting in millions in damage.[53]

Conclusions from International Diplomacy and Politics

The 2004 United Nations General Assembly Resolution 58/199 stands out as the most defining advocacy of a global cybersecurity culture and the protection of critical infrastructures. Resolution 58/199 invites all to "consider protecting critical information infrastructure in any future work on cyber security and within their respective national strategies and regulations and international cooperation."[54] The 2010 GGE report furthered the discussion, recommending "dialogue on norms for State use of ICTs to reduce risk and protect critical infrastructure."[55] In an ENISA analysis of numerous national security strategies, a common theme emerged, that of identifying and protecting critical infrastructure.[56] The Organization of American States communicated the need to develop and implement a cyber strategy against demonstrated threats to critical infrastructure.[57] The OSCE also strongly advises states to "reduce the risks of misperception, tension, and conflict" to "protect national and international critical infrastructures, including their integrity."[58]

James Lewis of the Center for Strategic and International Studies considered the high risks and proposed that countries should consider "pledging to avoid attacks." He also suggested that international norms of behavior could "stigmatize" certain cyber weapons against critical infrastructure as weapons of mass destruction.[59] The concept of "ruling out" cyber attacks against critical infrastructure is a recommendation by the International Stability Advisory Board to the US Department of State that stated, "Norms might, for example, include ruling attacks on critical infrastructure . . . as being unacceptable."[60] The US National Research Council Committee on Deterring Cyber Attacks noted that such agreements "may establish rules limiting appropriate targets."[61] Some international law experts recommend that potential targets such as power grids, food supplies, and financial infrastructures be restricted from cyber attack in the same way civilian aircraft are restricted from attack under all circumstances and all cyber war activities be restricted to the use of force in armed conflict.[62] Finally, the International Committee of the Red Cross (ICRC) has stated that international law has "already established a rule that forbids attacks on civilian infrastructure, even in cyberspace."[63]

The strongest persuasive argument for this norm of behavior toward critical infrastructure would be the United States' practice and unilateral actions during times of crisis and war. Examples would include the US decision not to hack into financial systems during Operation Allied Force and the Global War on Terror. Also, there was restraint against hacking the Iraqi financial system in 2003.[64]

Despite all of this, the actualization of norms against cyber attacks against critical infrastructure will likely center on the laws of armed conflict and the debates that will be generated. The United States has already asserted that "the United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of its choosing."[65] A "zone of ambiguity" remains with regard to exploitation, attack, and espionage in cyberspace that will have to be closed for full development of global norms or treaties protecting critical infrastructure.[66]

Significant Deficiencies in Critical-Infrastructure Security

Ponemon Institute surveyed 599 global IT and IT security executives in 13 countries in 2014.[67] The SANS Institute surveyed 268 respondents in 2014 who maintain, operate, or provide consulting services to industrial control systems.[68] Finally, the ENISA in 2011 surveyed 47 ICS operators and various academic, industrial standardization, and public actors.[69] These surveys included US companies, but the results are global in nature. There were three common themes—current security measures and training, risk awareness, and management influence.

Survey analysis indicated additional efforts are required to improve security measures and training. Ponemon found that only 17 percent of respondents reported that their IT security program is "mostly deployed," and only 50 percent reported their security measures are fully defined. Just 57 percent responded that their training programs were fully implemented. Significantly, only 43 percent said their security operations are committed to protecting the nation's critical infrastructure.[70] SANS reports that 67 percent considered or somewhat considered cybersecurity in their procurement process.[71]

Risk awareness remained a work in progress. Ponemon reported that 67 percent of respondents had at least one security compromise that affected operations or compromised confidential information. Also, only 16 percent were "fully aware" of vulnerabilities to ICS/SCADA, but 48 percent reported "fully aware" or "partially aware."[72] SANS reported that 53 percent of respondents believed there is a high to severe threat to their ICS systems, but only 26 percent believed their visibility to threats is excellent to good.[73] Furthermore, 40 percent believed or suspected that their ICS systems had been breached.[74] Seventeen percent had no process in place to detect vulnerabilities.[75]

Top-level management involvement in ICS security appeared to be lacking. Ponemon reported that only 28 percent of respondents believed that security is in the top five of their respective organization's strategic priorities. While many of these survey respondents represented large organizations, 55 percent reported that there was only one person responsible for ICS and SCADA security.[76] ENISA reported in its analysis that there is not enough involvement by senior management and that the excessive size and interests of some organizations preclude the sharing of security information.[77]

Counterarguments for a Critical-Infrastructure Protection Agreement

There are strong counterarguments for the establishment of an international norm or treaty. First, the very technical nature of cyberspace and the constantly evolving industrial systems could make a successfully negotiated treaty obsolete after years of development due to the innovative, offensive nature of cyber attacks.[78] Second, nations enter agreements to limit arms to maintain a "balance of power" and save on defense expenditures, but cyber-capability costs are extremely low in comparison. Nonstate actors would be unaffected by the agreement and might be (or might continue to be) used as proxies.[79] Third, the complexity of verification between private and public networks may be too difficult to overcome, in particular with some states' extreme reluctance to allow external access to their networks.[80] Fourth, according to a 1999 Department of Defense report, it might be more humane and preferred—regarding the laws of armed conflict—to target critical infrastructure with cyber weapons rather than using more traditional weapons that could increase civilian casualties and increase disruptions.[81] Finally, the problem of distinction between public and private networks may be unsolvable because 98 percent of all US federal networks travel on civilian infrastructure, and the laws of armed conflict could require a distinct, separate network be established to comply with an international norm.[82]

Regulatory and Legislative Improvement Debate

Highlights from Recent US Legislative and Regulatory Actions

The United States has made incremental improvements in the legislative and regulatory aspects of cybersecurity, but additional efforts to increase the regulatory powers of the federal government could increase critical-infrastructure protection. The champions of cybersecurity have found it difficult to pass legislation to implement measures that strengthen the government's oversight and regulatory powers. The proposed *Cybersecurity Act of 2012* was defeated in the Senate due to perceived costs to industry imposed by the new draft standards.[83] The H.R. 2952 Critical Infrastructure Research and Development Advancement Act of 2013, passed by the House of Representatives in July 2014, mandated the DHS submit a strategic plan and guide research and development efforts for protecting the critical infrastructure.[84] However, this law did not pass the Senate; a slimmed-down version became the National Cybersecurity Protection Act of 2014 in December 2014 that "codifies the existing cybersecurity and communications operations center at the Department of Homeland Security."[85]

Nathan Alexander Sales, a professor at George Mason University School of Law, provides an excellent summary of the regulatory and legislative initiatives to bolster the cybersecurity of the United States in "Regulating Cyber

Security." Professor Sales recommends that the United States view cybersecurity through the lens of environmental law and introduce regulations to shift the costs of vulnerabilities more specifically to the owners of critical infrastructure to improve accountability.

Currently, the majority of costs for breaches of poor cyber defenses are borne by the customers of critical infrastructure—underfunding of the nation's infrastructure defenses shifts seems to financial risk to customers.[86] Second, cyber defenses should be viewed through a public health lens that stresses the reporting of defects, detections, attacks, and treatment of national network systems.[87] As with Ebola or other pandemics, additional vigorous monitoring may bolster defenses by quickly isolating infected systems, regulating the need for redundancy, and hardening critical-infrastructure systems.[88]

Regulatory Conclusions from the Critical-Infrastructure Actors

Survey results of critical-infrastructure actors suggest a lean towards organizational self-interest. According to ENISA, only 4 percent of respondents believed that increased regulations would improve ICS security, yet 91 percent believed that public funding would be beneficial to ICS security due to the interests of governments and the public.[89] ICS manufacturers and operators tended to dislike more regulations, but service and security providers and academics supported increased regulation to improve security.[90] Surveys consistently noted concerns of increased regulation that may improve compliance but not necessarily security.[91] Although there was some disagreement about costs, only 15 percent of ICS manufacturers and integrators consider the costs of increased regulation unaffordable.[92] One survey result the surveyors found notable and surprising was that European ICS operators are familiar with US regulations and standards, despite their nonapplicability to their European ICS systems.[93] SANS and ENISA reported that many common standards are US-based and note the industry agrees that the European Union lacks a common reference to standards and guidelines.[94] A conclusion could be made that the United States is a perceived leader in the ICS security environment.

Recommendations

The global connections of the United States strengthen economic growth and provide tremendous benefits to the international society.[95] However, this interdependence creates risks that cannot be eliminated completely, especially if the offensive cyber capabilities of states and nonstate actors are perceived to have natural advantages in cost, maneuverability, and initiative.[96]

An important international cyber focus of the United States should be to reduce the risk to the nation's critical infrastructure, our strategic national assets. Analyses of surveys seem to indicate that there remains a significant lack of accountability and focus on critical-infrastructure cybersecurity that requires additional actions in support of the nation's *National Security Strategy*.

Recommendations are twofold:

- More emphasis should be placed on the development of international norms of cyber behavior and possibly an international treaty system in diplomacy to protect critical infrastructures from cyber attack. This process should take place outside the freedom of information debate. The issues of attribution and verification to such an agreement are potentially unsolvable. However, even a "symbolic" international agreement—even if *only* symbolic—may reduce the risk somewhat and provide maneuver room for continuous improvement of defensive measures.[97] An agreement of this type would potentially reduce risk *and* move toward an establishment of cyber norms. The United States should continue to resolve the ambiguities of developing norms and the laws of armed conflict.
- The United States should continue to make regulatory and legislative changes to improve the cybersecurity of the United States. Efforts should be made to harmonize US cybersecurity regulations and laws with the rest of the international community to enhance accountability and bolster international cyber defense. There seems to be a broad consensus on the need to improve critical-infrastructure cybersecurity, but the lack of accountability reduces the necessary funding and impedes the development of standards necessary to meet the objectives of the *National Security Strategy*.

Conclusion

Sixty-seven percent of industrial control system actors reported security compromises to their networks that included disruption to operations or losses of confidential information.[98] Threats to the nation's infrastructure are now more unlimited, enigmatic, and pervasive. The 2010 *National Security Strategy* acknowledges threats to critical infrastructure and seeks a path forward with international partners to craft norms of good state behavior, but the United States promotes values such as the freedom of information and access that create international disagreements and frustrates diplomatic efforts.[99] Nonetheless, the effort to develop international norms that specifically relate to critical-infrastructure security is coherent and prevalent throughout the world community. Focusing on the areas of consensus about the protection of critical infrastructure may be the most feasible way to achieve cyber norms or treaty systems in the current international environment. Also, domestic legislative and regulatory initiatives could reduce the risks to the nation's digital systems that empower the critical infrastructure of the United States and strengthen our cyber defenses.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Panetta, Secretary of Defense, *Remarks on Cybersecurity*.

2. King, "Cyberattack on German Iron Plant."

3. President, *National Security Strategy*, 18–22.

4. Yannakogeorgos, "Cyberspace."

5. Clinton, *Remarks on Internet Freedom*; President, *International Strategy for Cyberspace*, 5; and "Letter dated 12 September 2011 from the Permanent Representatives," United Nations General Assembly.

6. President, *National Security Strategy*, 8, 27, 50.

7. Ibid., 18, 27.

8. President, Presidential Decision Directive 63 on Critical Infrastructure Protection; and President, *International Strategy for Cyberspace*.

9. US Department of Homeland Security, *National Infrastructure Protection Plan*; and Chen, *Assessment of the Department of Defense Strategy*, 6–8; and US Department of Defense, "Department of Defense Strategy for Operating in Cyberspace."

10. Press release. *Executive Order*.

11 President, *International Strategy for Cyberspace*, 3, 8–11, 5.

12 "Letter dated 12 September 2011 from the Permanent Representatives," A/66/359, United Nations General Assembly.

13. *Developments in the Field of Information and Telecommunications*, Resolution 53/70, United Nations General Assembly; and Lewis, "Liberty, Equality, Connectivity," 11.

14. United Nations, *Group of Governmental Experts*, United Nations General Assembly, 30 July 2010.

15. "Letter dated 12 September 2011 from the Permanent Representatives," United Nations General Assembly; and Aritmatsu, "Treaty for Governing Cyber Weapons," 91.

16. Ford, "Trouble with Cyber Arms Control," 59.

17. Giles, "Russia's Public Stance on Cyberspace Issues," 65; Markoff and Kramer, "In Shift, US Talks to Russia on Internet Security"; and Maurer, *Cyber Norm Emergence at the United Nations*, 17.

18. Ford, "Trouble with Cyber Arms Control," 62–63; and Swaine, "Chinese Views on Cybersecurity in Foreign Relations," 3.

19. Ford, "Trouble with Cyber Arms Control," 65; and Hsu and Murray, *China and International Law in Cyberspace*, 1.

20. Hsu and Murray, *China and International Law in Cyberspace*, 3.

21. President, *International Strategy for Cyberspace*.

22. Chen, *Assessment of the Department of Defense Strategy*, 24.

23. US Department of State, International Security Advisory Board, *Report on Framework for International Cyber Stability*, 15.

24. Nye, *Cyber Power*, 18; Maurer, *Cyber Norm Emergence at the United Nations*, 25; and Aritmatsu, "Treaty for Governing Cyber Weapons," 95.

25. "Letter dated 12 September 2011 from the Permanent Representatives," United Nations General Assembly. 3.

26. Ibid., 4–5.

27. Clarke, *Securing Cyberspace through International Norms*, 4.

28. Convention on Cybercrime, Council of Europe European Treaty Series No. 185. Limited in scope to criminal matters and mostly to Europe, the Convention on Cybercrime (COE) came into force in 2004 stating that, "The Parties should co–operate with each other" through international instruments in criminal matters and on the basis of legislation and domestic laws. The COE was signed and ratified by the United States and referenced in the International Strategy for Cyberspace for its support to international law enforcement agencies, due process, and the rule of law in cyberspace.

29. Sofaer, Clark, and Diffie, "Cyber Security and International Agreements," 180.

30. Goldsmith, *Cybersecurity Treaties*, 7.

31. Clarke and Knave, *Cyber War*; and Sofaer, "Cyber Security and International Agreements," 192.

32. Yannakogeorgos and Lowther, "Prospects for Cyber Deterrence," 66.

33. Sofaer, Clark, and Diffie, "Cyber Security and International Agreements," 192; and United Nations, *Report of the Group of Governmental Experts*, General Assembly, sixty-fifth session, 30 July 2010.

34. Lewis, "Liberty, Equality, Connectivity," 4.

35. Ibid, 5; and United Nations, *Report of the Group of Governmental Experts*, General Assembly, sixty-sixth session, 24 June 2013.

36. Joint Publication 3-13 (R), *Cyberspace Operations*, III-10. This complies with Organization for Security and Cooperation in Europe confidence-building measure 7, Organization for Security and Cooperation in Europe (OSCE), Permanent Council Decision No. 1106, *Initial Set of OSCE Confidence Building Measures*, 2.

"Participating States will voluntarily share information on their national organization; strategies; policies and programs—including on cooperation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties."

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-12: Cyberspace Operations," 28.

37. OSCE, Permanent Council Decision No. 1106, *Initial Set of OSCE Confidence Building Measures*, 1.

38. Ibid., Interpretative Statement under Paragraph IV.1(A)6 of the Rules of Procedure of the Organization for Security and Co-Operation in Europe (Russian Interpretative Statement).

39. US Mission to the Organization for Security and Cooperation in Europe. "US Welcomes Cyber Security Showcase."

40. President, *International Strategy for Cyberspace*, 5; and US Department of State, International Security Advisory Board. *Report on Framework for International Cyber Stability*, 20.

41. NETmundial Initiative, *Netmultistakeholder Statement*.

42. Organization for Security and Cooperation in Europe (OSCE), Permanent Council Decision No. 1106, *Initial Set of OSCE Confidence Building Measures*, 2.

43. President, *International Strategy for Cyberspace*, 8.

44. Hsu and Murray, *China and International Law in Cyberspace*, 2; and Giles, "Russia's Public Stance on Cyberspace Issues," 66.

45. United Nations, *Universal Declaration of Human Rights*.

46. United Nations, *Report of the Special Rapporteur*, General Assembly, sixty-sixth session, 10 August 2011.

47. Lewis, "Liberty, Equality, Connectivity," 6.

48. European Network and Information Security Agency (ENISA), *Protecting Industrial Control Systems,* 1.

49. Ibid, 5.

50. Flowers, Zeadally, and Murray, "Cybersecurity and US Legislative Efforts," 30.

51. US Department of Homeland Security, *Critical Infrastructure Sector Partnerships*.

52. Minkel. "2003 Northeast Blackout"; "Great 2003 Northeast Blackout and $6 Billion Software Bug," *Availability Digest* (March 2007): 2–4, http://www.availabilitydigest.com/private/0203/northeast_blackout.pdf; and McConnell, "Cyber Insecurities," 36.

53. Schroeder, "The Unprecedented Economic Risks of Network Security," 170.

54. *Creation of a Global Culture of Cybersecurity*, resolution 58/199.

55. United Nations, *Report of the Group of Governmental Experts*, General Assembly, sixty-fifth session, 30 July 2010.

56. ENISA, "National Cyber Security Strategies."

57. Organization of American States, AG/RES. 2004, *Adoption of a Comprehensive Inter–American Strategy*.

58. Organization for Security and Cooperation in Europe (OSCE), Permanent Council Decision No. 1106, *Initial Set of OSCE Confidence Building Measures*, 1.

59. Lewis, "Liberty, Equality, Connectivity," 4.

60. US Department of State, International Security Advisory Board, *Report on Framework for International Cyber Stability*, 16.

61. National Research Council Committee on Deterring Cyber Attacks, *Letter Report for the Committee on Deterring Cyber Attacks*; and Sofaer, Clark, and Diffie, "Cyber Security and International Agreements," 192.

62. Sofaer, Clark, and Diffie, "Cyber Security and International Agreements," 193.

63. Rabkin and Rabkin, "Navigating Conflicts in Cyberspace," 231.

64. Maurer, *Cyber Norm Emergence at the United Nations*, 10; and Clarke, *Securing Cyberspace through International Norms*, 25.

65. "Pentagon Unveils New Offensive Cybersecurity Strategy," *Radio Free Europe/Radio Liberty*; and Chen, *Assessment of the Department of Defense Strategy*, 12.

66. Mueller, *Laws of War and Cyberspace*, 9.

67. Ponemon Institute. *Critical Infrastructure*. Ponemon Institute LLC surveyed 599 global IT and IT security executives in 13 countries. To ensure a knowledgeable and quality response, only IT practitioners whose job involves securing or overseeing the security of their organization's information systems or IT infrastructure were permitted to complete the survey. They were also familiar with security standards such as the North American Electric Reliability Corporation, critical infrastructure protection standards, National Institute of Standards and Technology, International Organization for Standardization, Peripheral Component Interface

Security Standards, Defense Security Service, Sarbanes Oxley, and other regulations on the protection of information assets and the critical infrastructure.

68. Luallen and Harp, *Breaches on the Rise in Control Systems*. Of the 268 survey respondents, more than 67 percent actively maintain, operate, or provide consulting services within facilities maintaining industrial control systems, with most of the remaining ("Other" category) providing educational, legal, and government services to this industry. The energy/utilities (23 percent) and oil and gas (11 percent) industries accounted for the largest number of participants. Nearly 64 percent of the survey participants work in businesses with more than 1,000 employees, and 30 percent of the participants operate in businesses with more than 15,000 personnel.

69. ENISA, *Protecting Industrial Control Systems*, 11. ENISA surveyed ICS software/hardware manufacturers and integrators, ICS security tools and service providers, infrastructure operators, academia, R&D, public officials, and standardization professionals to include 20 personal interviews.

70. Ponemon Institute. *Critical Infrastructure*, 2, 4, 7.

71. Luallen and Harp, *Breaches on the Rise in Control Systems*, 21.

72. Ponemon Institute. *Critical Infrastructure*, 3, 10.

73. Luallen and Harp, *Breaches on the Rise in Control Systems*, 6, 8.

74. Ibid., 10.

75. Ibid., 1.

76. Ponemon Institute. *Critical Infrastructure*, 2, 8.

77. ENISA, *Protecting Industrial Control Systems*, Annex II, "Survey and Interview Analysis," 5, 8.

78. Rabkin and Rabkin, "Navigating Conflicts in Cyberspace," 257.

79. Aritmatsu, "Treaty for Governing Cyber Weapons," 100.

80. Ibid., 101.

81. Aritmatsu, "Treaty for Governing Cyber Weapons," 104; and Kanuck, "Sovereign Discourse on Cyber Conflict," 1595.

82. Aritmatsu, "Treaty for Governing Cyber Weapons," 106; and Sales, "Regulating Cyber Security," 1524.

83. Flowers, Zeadally, and Murray, "Cybersecurity and US Legislative Efforts to Address Cybercrime." 13.

84. US House, *Critical Infrastructure Research and Development Advancement Act*. This version was reported to House, 1 September 2014, and passed by the House of Representatives in 2014 before amendments by the US Senate.

85. Kimery, "Congress Approves Cybersecurity Legislation"; and Cybersecurity Workforce Assessment Act, Public Law No: 113–246.

86. Sales, "Regulating Cyber Security," 1525–1528.

87. Ibid., 1509.

88. Ibid.

89. ENISA, *Protecting Industrial Control Systems*, Annex II, 6, 26.

90. Ibid., 6.

91. Ibid., 18.

92. Ibid., 20.

93. Ibid., 12.

94. Luallen and Harp, *Breaches on the Rise in Control Systems*, 19; ENISA, *Protecting Industrial Control Systems*, annex II, 11; and ENISA, *Protecting Industrial Control Systems*, 14.

95. President, *National Security Strategy*, 50.
96. Sales, “Regulating Cyber Security,” 1545.
97. Ford, “Trouble with Cyber Arms Control,” 53.
98. Ponemon Institute. *Critical Infrastructure*, 3.
99. President, *National Security Strategy*, 3, 5.

Appendix

Excerpts from: "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," A/66/359, UN General Assembly, 4–5.

Purpose and scope

The purpose of the present code is to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviors and enhance their cooperation in addressing the common threats and challenges in information space, so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people's well-being, with the objective of maintaining international stability and security.

Adherence to the code is voluntary and open to all States.

Code of conduct

Each State voluntarily subscribing to the code pledges:

(a) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries;

(b) Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies;

(c) To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment;

(d) To endeavor to ensure the supply chain security of information and communications technology products and services, in order to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of the countries that have accepted the code of conduct, to gain independent control of information and communications technologies or to threaten the political, economic and social security of other countries;

(e) To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage;

(f) To fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations;

(g) To promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet;

(h) To lead all elements of society, including its information and communication partnerships with the private sector, to understand their roles and responsibilities with regard to information security, in order to facilitate the creation of a culture of information security and the protection of critical information infrastructures;

(i) To assist developing countries in their efforts to enhance capacity building on information security and to close the digital divide;

(j) To bolster bilateral, regional and international cooperation, promote the important role of the United Nations in formulating international norms, peaceful settlements of international disputes and improvements in international cooperation in the field of information security, and enhance coordination among relevant international organizations;

(k) To settle any dispute resulting from the application of the code through peaceful means and to refrain from the threat or use of force.

Bibliography

Aritmatsu, Louise. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations." In *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis and K. Ziolkowski, 91–106. Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence Publications, 2012.
https://ccdcoe.org/cycon/2012/proceedings/d3r1s6_arimatsu.pdf (accessed 15 Feb 2015).

Chen, Thomas. *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*. The Letort Papers. Carlisle Barracks, PA: Strategic Studies Institute, September 2013.
http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1170.pdf.

Clarke, Richard A., *Securing Cyberspace through International Norms: Recommendations for Policymakers and the Private Sector*. Good Harbor Security Risk Management, n.d.
http://www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf.

Clarke, Richard A., and Robert K. Knave. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Harper Collins, 2010.

Clinton, Hillary Rodham, US Secretary of State. *Remarks on Internet Freedom at the Newseum*. US Department of State, 21 January 2010. http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

Convention on Cybercrime. Council of Europe European Treaty Series No. 185, 23 November 2001. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-12: Cyberspace Operations," 30 November 2011. https://doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf.

Cybersecurity Workforce Assessment Act. Public Law 113-246. 113th Cong., 1st Session, 18 December 2014. https://www.congress.gov/bill/113th-congress/house-bill/2952/text.

Developments in the Field of Information and Telecommunications in the Context of International Security. Resolution 53/70. United Nations General Assembly, 53rd session, 4 January 1999. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70.

European Network and Information Security Agency. "National Cyber Security Strategies," 8 May 2012. https://www.enisa.europa.eu/publications/cyber-security-strategies-paper/at_download/fullReport.

———. *Protecting Industrial Control Systems, Recommendations for Europe and Member States*, 9 December 2011. https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport.

Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US Legislative Efforts to Address Cybercrime." *Journal of Homeland Security and Emergency Management* 10, no. 1 (April 2013): 29–55.

Ford, Christopher A. "The Trouble with Cyber Arms Control." *The New Atlantis, A Journal of Technology and Society* 29 (Fall 2010): 53–67. http://www.thenewatlantis.com/docLib/20110301_TNA29Ford.pdf.

Giles, Keir. "Russia's Public Stance on Cyberspace Issues." In *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolkowski, 65–66. Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence Publications, 2102. https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

Goldsmith, Jack. *Cybersecurity Treaties, A Skeptical View*. Koret-Taube Task Force on National Security and Law, Stanford, CA: Hoover Institution, Stanford University, February 2011. http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

Highleyman, Bill. "The Great 2003 Northeast Blackout and the $6 Billion Software Bug." *The Availability Digest*, March 2007. http://www.availabilitydigest.com/private/0203/northeast_blackout.pdf.

Hsu, Kimberly, and Craig Murray. *China and International Law in Cyberspace*. US-China Economic and Security Review Commission, 6 May 2014. http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf.

International Committee of the Red Cross (ICRC). "Cyber Warfare." ICRC, 29 October 2010. http://www.icrc.org/eng/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm.

Joint Publication 3-13 (R), *Cyberspace Operations*. 5 February 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Kanuck, Sean. "Sovereign Discourse on Cyber Conflict under International Law," *Texas Law Review* 88, no. 7 (June 2010): 1571–97. https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Kanuck.pdf.

Kimery, Anthony. "Congress Approves Cybersecurity Legislation." *Homeland Security Today*, 11 December 2014. http://www.hstoday.us/briefings/daily-news-analysis/single-article/congress-approves-cybersecurity-legislation/dcca3f20b55482c5fc6e2fcc4535e914.html.

King, Rachael. "Cyberattack on German Iron Plant Causes 'Widespread Damage': Report," *The Wall Street Journal*, 18 December 2014. http://blogs.wsj.com/cio/2014/12/18/cyberattack-on-german-iron-plant-causes-widespread-damage-report/.

"Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." A/66/359. United Nations General Assembly. https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

Lewis, James A. "Liberty, Equality, Connectivity—Transatlantic Cooperation on Cybersecurity Norms." Center for Strategic and International Studies, February 2014. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140225_Lewis_TransatlanticCybersecurityNorms.pdf.

Lord, Kristin M., and Travis Sharp, eds. *America's Cyber Future Security and Prosperity in the Information Age*. Vol. 2. Washington, DC: Center for a New American Strategy, June 2011. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf.

Luallen, Matthew, and Derek Harp. *Breaches on the Rise in Control Systems: A SANS Survey publication*. SANS Institute, April 2014. http://www.sans.org/reading-room/whitepapers/analyst/breaches-rise-control-systems-survey-34665.

Markoff, John, and Andrew E. Kramer. "In Shift, US Talks to Russia on Internet Security." *New York Times*, 12 December 2009. http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0.

Maurer, Tim. *Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-Security*. Discussion Paper 2011-11. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

McConnell, Mike. "Cyber Insecurities: The 21st Century Threatscape." In *America's Cyber Future Security and Prosperity in the Information Age*. Vol. 2. Edited by Kristin M. Lord and Travis Sharp, 27–39. Washington DC: Center for a New American Strategy, June 2011. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf.

Minkel, J. R. "The 2003 Northeast Blackout—Five Years Later." *The Scientific American*, 13 August 2008. http://www.scientificamerican.com/article/2003-blackout-five-years-later/.

Mueller, Benjamin. *The Laws of War and Cyberspace: On the Need for a Treaty Concerning Cyber Conflict*. Strategic Update 14.2. London: The London

School of Economics and Political Science, June 2014. http://www.lse.ac.uk/IDEAS/publications/reports/pdf/SU14_2_Cyberwarfare.pdf.

National Research Council Committee on Deterring Cyber Attacks. *Letter Report for the Committee on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*. Washington, DC: The National Academies Press, 25 March 2010. http://www.nap.edu/catalog/12886.html.

NETmundial Initiative. *Netmultistakeholder Statement*. NETmundial Initiative, 24 April 2014. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Nye, Joseph S. Jr. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Organization for Security and Cooperation in Europe (OSCE). Permanent Council Decision No. 1106. *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, 3 December 2013. http://www.osce.org/pc/109168.

Organization of American States. AG/RES. 2004 (XXXIV). *Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, 8 July 2004. https://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf.

Panetta, Leon E. Secretary of Defense. *Remarks on Cybersecurity to the Business Executives for National Security*. US Department of Defense, 11 October 2012. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

"Pentagon Unveils New Offensive Cybersecurity Strategy." *Radio Free Europe/Radio Liberty*, 15 July 2011. www.rferl.org/content/pentagon_unveils_new_offensive_cybersecurity_strategy/24266548.html.

Ponemon Institute. *Critical Infrastructure: Security Preparedness and Maturity*. Unisys, July 2014. http://www.unisys.com/insights/critical-infrastructure-security.

President. *International Strategy for Cyberspace*. The White House, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. *National Security Strategy*. The White House, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

———. *The National Strategy to Secure Cyberspace*. February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Presidential Decision Directive 63. Critical Infrastructure Protection: Sector Coordinators, 5 August 1998. http://www.gpo.gov/fdsys/pkg/FR-1998-08-05/html/98-20865.htm.

Press release. *Executive Order—Improving Critical Infrastructure Cybersecurity*. The Whitehouse, 12 February 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

Rabkin, Jeremy, and Ariel Rabkin. "Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea." *Chicago Journal of International Law* 14, no 1 (Summer 2013): 197–257.

Sales, Nathan Alexander. "Regulating Cyber-Security," *Northwestern University Law Review* 107, No. 4 (Summer 2013): 1503–68. http://www.law.northwestern.edu/lawreview/issues/107.4.html.

Schroeder, Christopher M. "The Unprecedented Economic Risks of Network Insecurity." In *America's Cyber Future Security and Prosperity in the Information Age*. Vol. 2, edited by Kristin M. Lord and Travis Sharp, 167–81. Washington, DC: Center for a New American Strategy, June 2011. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf.

Sofaer, Abraham D., David Clark, and Whitfield Diffie. "Cyber Security and International Agreements." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, 179–92. Washington DC: National Academies Press, 2010. http://nap.edu/12997.

Swaine, Micheal D. "Chinese Views on Cybersecurity in Foreign Relations." *China Leadership Monitor* 42 (Fall 2013). http://www.hoover.org/sites/default/files/uploads/documents/CLM42MS.pdf.

United Nations. *Report of the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security*. General Assembly, 65th session, 30 July 2010. http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201.

———. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. General Assembly, 68th session, 24 June 2013. http://undocs.org/A/68/98.

———. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. General Assembly, 66th session, 10 August 2011. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/449/78/PDF/N1144978.pdf.

———. *Universal Declaration of Human Rights: 60th Anniversary Special Edition, 1948–2008*. 10 December 2008. http://www.ohchr.org/EN/UDHR/Documents/60UDHR/bookleten.pdf.

United Nations General Assembly. Resolution 58/199: *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, 20 January 2004. www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

US Mission to the Organization for Security and Cooperation in Europe. "US Welcomes Cyber Security Showcase Highlighting Confidence Building Measures," 7 November 2014. https://osce.usmission.gov/u-s-welcomes-cyber-security-showcase-highlighting-confidence-building-measures/.

US Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*, July 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

US Department of Homeland Security (USDHS). *Critical Infrastructure Sector Partnerships*. USDHS, 27 October 2015. https://www.dhs.gov/critical-infrastructure-sector-partnerships.

———. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, 2009. https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

US Department of State, International Security Advisory Board (ISAB). *Report on a Framework for International Cyber Stability*. ISAB, 2 July 2014. http://www.state.gov/documents/organization/229235.pdf.

US House. *Critical Infrastructure Research and Development Advancement Act of 2013*. 113th Congress, 2nd session, 2014. HR 2952.

Yannakogeorgos, Panayotis A. "Cyberspace: The New Frontier—and the Same Old Multilateralism." In *Global Norms, American Sponsorship and the Emerging Patterns of World Politics,* edited by Simon Reich, 147–77. New York: Palgrave–Macmillan, 2010.

Yannakogeorgos, Panayotis A. and Adam B. Lowther. "The Prospects for Cyber Deterrence: American Sponsorship of Global Norms." In *Conflict and Cooperation in Cyberspace, The Challenge to National Security*, edited by Panayotis A. Yannakogeorgos and Adam B. Lowther, 49–81. Boca Raton, FL: Taylor and Francis, 2014.

AIR FORCE RESEARCH INSTITUTE

AUP
AIR UNIVERSITY PRESS

http://aupress.au.af.mil

ISBN 978-1-58566-266-1
ISSN 2329-5821