Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):28-37
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

INTERNATIONAL CYBER SECURITY CHALLENGES AND SCADA SYSTEMS

Tinatin Mshvidobadze
Gori State University

ABSTRACT

The development and application of the information and communications technology has created a new battleground. Cyber security will significantly affect international relations in the 21st century. This paper gives an overview of the concepts and principles of cyber threats that affect the safety and security in an international context.

It is shown the state of the art in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. The discussion begins with an examination of what constitutes critical national infrastructure and the roles of ICS and SCADA systems within it. The examination also touches on the political and social challenges in achieving greater cyber security, and then shifts to a description of how the US government divides efforts among its lead cyber security agencies and what responses to a cyber attack on ICS or SCADA might look like. The discussion finishes with recommendations for strengthened international consensus on norms for state behavior, formalized public-private relationships, and interagency efforts to realize a more secure and resilient national infrastructure.

KEYWORDS: cyberspace, cyber-attack, cyber terrorism and crime, international security.

Cyber-attacks on infrastructure

We now live in a world where warfare can be conducted entirely virtually – though the consequences will almost always have repercussions in the physical world.

As we integrate technology further into our lives, the opportunities for abuse grow. So too, then, must the defenses we employ to stop them through the education and practice of cyber security.

AS societies around the world defend ever more heavily on technology, the ability to shut down or destroy infrastructure, take control of machines and vehicles, and directly cause the loss of life has become a reality. To date, some of the more well-known examples of cyber-attacks on infrastructure include:

• In 2008 when Russia sent tanks into Georgia, the attack coincided with a cyber-attack on Georgian government computing infrastructure. This is thought to be one of the first land and cyber coordinated attacks [1].

• Also in 2008, Stuxnet – a computer worm purportedly jointly designed by the US and Israel – crippled Iran's nuclear-enrichment program by sabotaging centrifuges [2].

• In 2014 a German steelwork was disabled and a furnace severely damaged when hackers infiltrated its networks and prevented the furnace from shutting down [3].
• In 2015, with an attack strongly suspected to have originated from Russia, 230,000 people lost power when 30 sub-stations in Western Ukraine were shut down via a remote attack [4].
In all of these, and as an indication of how the landscape of war is changing, the weapon of choice for these attacks wasn't guns or bombs – it was a keyboard.
French Coldwell, Chief Evangelist at governance, risk, and compliance apps company Metricstream, at a cyber-security summit earlier this year noted that "this is the canary in the coalmine. Much more of this will come" [5].
We can expect governments around the world to strengthen their cyber-attack and defense capabilities, spurring an arms race that will operate at a much faster pace than we saw in the Cold War. But here the results could be much subtler – as noted in the McAfee 2016 Threats Predictions report, "they will improve their intelligence-gathering capabilities, they will grow their ability to surreptitiously manipulate markets, and they will continue to expand the definition of and rules of engagement for cyber warfare." [6]

International cyber security

Cyber warfare and terrorism do not know borders. Action in cyberspace requires the rejection of the common assumptions related to time and space because such attacks, by means of modern information and communications networks, can be performed from anywhere in a very short time. The processes of globalization did not have the impact only on the achievements of civilization, but also on the development of new threats to the civilization.
The initial hypothesis is that cyberspace is a growing security risk and challenge of modern times. Moreover, cyber security will significantly affect international relations in the 21st century, while the threats and challenges will exponentially increase.
The scientific work seeks to show cyberspace as an operational dimension of international relations in terms of the cyber security challenges. With the systematization of the cyber warfare strategy and the very methods of attack, links with the planned action will be set up through the application of technical, computing and network systems.
The new, cyber dimension of international relations is a major challenge for the theories of the preservation of power and intimidation. Cyber threats are serious, destabilizing and on the increase. The theories and strategies of intimidation designed and implemented during the Cold War cannot be implemented in the cyber domain. Many scientists are working on the understanding of the cyber revolution in international relations.
Authorities have also taken certain steps in cooperation, especially in the area of crime and the establishment of CERTs (Computer Emergency Response Teams) [7]. Tatalović, Grizold and Cvrtila write that the processes of internationalization and globalization have brought a greater cohesion and efforts for a unified regulation of the world order, more than it was in the system of sovereign states during the Cold War. This is reflected in the core of the states' security policies. In that context, a new concept – human security concept – emerged in theory and political practice. In contrast to the traditional concept of national security, it primarily emphasizes the security of an

individual, not the state [8]. Lin theorizes [9] about cyber security. The concept of intimidation was the basic idea of the nuclear strategy. Even though nuclear and cyber weapons share a key feature – the superiority of the attack in comparison with the defense – they differ in many ways. Experts and analysts estimate that the efforts of Russia and China to dominate cyberspace have over the past few years intensified so much that any delay in this area could present a big problem for the modern West.

Cyber-attack, whether it happens as a conflict between states, a terrorist or a criminal act, is an attack in cyberspace with the aim of compromising a computer system or network, but also of compromising physical systems as it was the case with the Stuxnet worm. In layman's, popular terms, most often mentioned in the media, it is called a hacker attack. Identical methods of a hacker attack are applied for both military and terrorist purposes.

Janczewski and Colarik [10] divided cyber-attacks into phases, which they consider to be basically the same as the phases of conventional criminal offenses:

• the first phase of the attack is the scouting of potential victims. By observing the implementation of the normal operations of targets, useful information that are accumulated and determined through the used applications and hardware;

• the second phase of the attack is intrusion. Until the attacker gets into the system, there is not much that can be done against the target apart from disrupting the availability or access to certain services provided by the target;

• the next phase is the identification and dissemination of internal opportunities by examining the resources and the right to access the restricted and important parts of the system;

• in the fourth phase the intruder does damage to the system or steals certain data.

In such circumstances of transformation and different views and understandings of security in general and international security, cyber threats certainly redefine those terms. In line with the efforts to ensure security on one hand and specificities of cyber threats and motives of the actors who initiate them on the other, it will be necessary to set up a new international security paradigm of the cyber age.

SCADA systems and cyber security challenges

A SCADA system consists of hardware and software components, and of a connecting network(s). Fig. 1 shows a generic hardware architecture of a SCADA system. An architecture is formed by one or more control centers and a number of field devices such as an RTU, Intelligent Electronic Device (IED) and Programmable Logic Controller (PLC) connected by a communication infrastructure. An RTU receives data from field devices, converts it to digital data and sends it to the control centre as well as receives digital commands from the centre and handles alarms. A PLC is a digital computer that monitors sensors and takes decisions based upon a user created program to control valves, solenoids and other actuators. A control centre includes an MTU, which issues commands to and gathers data from RTUs, it also stores and processes data in order to display information to human operators to support decision making.

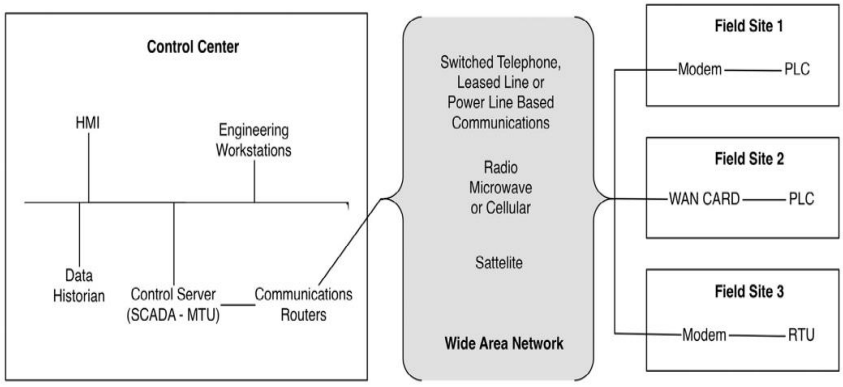

Fig. 1 – Generic SCADA hardware architecture. NIST SP 800-82

In reality, security goals, in whatever order they appear, are often preceded in SCADA systems by safety, reliability, robustness and maintainability (which are the supreme goal of critical systems) leaving little or no resources for security goals. In Park and Lee [11], the authors discuss a need for an update of such well-established international security standards as NIST SP 800-53 and ISO 27001 in order to address the specifics of ISC is stated. A new standard, according to Park and Lee, shall bring together the CIA-traid and safety requirement critical in the context of an ICS.
Cyber security issues in SCADA systems are further exacerbated by the legacy problem. Existing SCADA systems, due to their continuous operation, are not updated or re-designed in some cases for decades. The nature of SCADA systems requires them to be operational 24 hours 7 days a week. This makes the regular patching and upgrading of both a SCADA software and a hosting operating system difficult, if not impossible. The patching of a SCADA system is complicated by the facts that the system is time-critical, there is no test environment and patching may introduce new unknown vulnerabilities or ultimately break the system. Legacy SCADA system may end up relying on operating systems and software that are no longer supported by vendors [12].

Risk assessment methods for SCADA Risk assessment, detection, and response, 2011
A risk assessment method for sensor networks accompanied by attack detection and automatic response modules is presented in Cardenas et al. [13]. In Cardenas et al. the standard formula for calculating risk as an average loss is accepted and interpreted in the context of a sensor network:

$$R_\mu = \sum_i L_i \; P_i \qquad (1)$$

where P_i is the probability of an attacker compromising sensor i and is accepted to be the same for all sensors and L_i is a loss resulting from the compromise.
The following attack model is proposed which may reflect integrity and DoS attacks:

$$\acute{y}_i\ (k) = \begin{cases} Y_i\ (k), & for k\ \notin \mathrm{K}_\alpha \\ a_i\ (k), & for\ k\ \in \mathrm{K}_\alpha, a_i\ (k) \in \gamma_a \end{cases} \quad (2)$$

where $\acute{y}_i\ (k)$ is a measurement received by the controller at time k; $Y_i\ (k)$, is an actual measurement; $a_i\ (k)$, is a measurement under attack; and K_α is the duration of an attack.

For detecting anomaly, a linear model as an approximation of the behavior of a physical system is developed. Then, anomaly is detected using a non-parametric cumulative sum statistic. When anomaly is detected, an automated response to an attack is fired while awaiting human actions. The experiments were run to simulate cyber attacks on a chemical reactor implemented as a Tennessee-Eastman process control system model presented in Ricker [14]. The experiments demonstrated that the risk assessment model proposed helps to establish which type of attack and which sensor in a network must be given a priority in a security budget.

Threat Trends

The opportunities for a cyber attack on SCADAs are replete with various methods and avenues of attack to achieve devastating effects on a target network.

The effects of data manipulation, instrument alteration, or power fluctuation upon an ICS or SCADA systems represent scenarios where cyber generates tangible effect upon businesses or governments. Points of attack may include an ICS, external office IT network, calibration tools, field devices, safety systems, technician support equipment, and even the employees themselves.

The national leadership attention provided to this problem set is directly proportional to the increased public reporting of compromises by both state and non state actors. There have been a startling number of reports recently, including a coordinated cyber intrusion into US pipeline SCADA systems, Russian hackers exploiting Western energy companies and ICSs in 23 countries, Chinese and Russian mapping of the US electrical grid, regional conflicts such as the Syrian civil war bleeding into cyberspace, and unknown hackers shutting down an oil platform by inducing unsafe tilting [15]. There is also growing speculation North Korea could capitalize on known vulnerabilities, and indications that Iranian actors "have directly attacked, established persistence in, and extracted highly sensitive materials from [major] critical infrastructure companies."[16]

Also, several recent and public cyber-attacks on ICSs or SCADAs have generated catastrophic results. The first publicly released and highly formative demonstration of ICS vulnerability was the Aurora Generator Test conducted by the Idaho National Laboratory in 2007, where the intentional and rapid opening and closing of breakers in a commercially available generator induced an out-of-phase condition that effectively destroyed the equipment when connected to the power grid[17].

Security experts extrapolate that the Aurora vulnerability is not merely constrained to generators but extends to electrical systems and rotating equipment elsewhere, such as in manufacturing, refineries, data centers, and mass transit.

In unprecedented official recognition of the threat to SCADA, Adm Michael Rogers, US Navy, director of the National Security Agency (NSA) and commander of US Cyber Command (USCYBERCOM), testified before Congress that "China and 'one or two' other countries are capable of mounting cyber attacks that would shut down the [US] electric grid and other critical

systems."[18]. Any uncertainty in whether the United States appreciates the gravity of this problem set is eliminated in the clearest terms of EO 13636, as "it is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure.

Cyber Response

Cyber responses bearing both challenges and benefits is discussed below. Without considering the means of employment, cyber responses will aim at one or more of the following:

• observe and gain intelligence;
• deny an attack's objectives through defense and hygiene;
• neutralize the attacker and impose a proportional cost on them, or
• retaliate with a high-order response to deter future attacks.

The means of responding could include:

• hacking adversarial command-and-control infrastructure;
• interrupting network protocols;
• luring attackers into honey pot traps;
• coordinating with computer security incident response teams (CSIRT) and Internet service providers (ISP) to disrupt malicious traffic, or
• applying cyber effects to facilities or services, like ventilation or power systems, attackers rely on to execute operations.

Cyberspace is different from other domains in the sheer speed of its activities. Therefore, any related consultative process, such as an emergency national response mechanism, has to be very streamlined and adaptive to respond within an adversary's observe-orient-decide-act (OODA) loop[19]. Additionally, access to and exploitation of "hard" targets in advanced nation-states, might take weeks or months to accomplish. Cross-domain or covert activities might be required before being able to hold adversaries at risk.

Prevention

I consider it appropriate to correct policy recommendations for synchronizing and prevention cyber security efforts.

The first line of effort is prevention, a pre conflict phase where the government can capitalize on the momentum already under way across various sectors and institutions. Prevention also requires complementary foreign and domestic initiatives including:

• international norms of cyber behavior;
• formalized critical interdependencies;
• private-sector responsibilities in law and regulation;
• focused research into advanced cyber capabilities, and
• cyber workforce professionalization.

The United States must strive to establish an international set of norms that define both peacetime and contingency expectations for state cyber behavior, communicate clear cyber foreign policy, pursue cyber defense capacity building measures with developing nations, and develop an international understanding of the nature of "critical infrastructure." Building an internationally

accepted framework of norms of behavior and confidence-building measures in cyberspace are foremost among these efforts. This framework will provide a new level of strategic stability in cyberspace and afford the US government freedom of action in cyberspace consistent with the nation's principles and interests. The interagency approved the draft cyber initiatives on peacetime norms in 2014[20]. The initiatives are intended for future international consideration and hold that states:

• should not perform cyber-enabled intellectual property theft for economic advantage;[21].
• should not attack or impair critical infrastructure;
• should not impede national computer-security-incident-response team actions;
• should behave consistently with domestic and international laws and obligations.

These norms depend upon utilizing traditional multi stakeholder Internet governance rather than state-administered models of cyberspace governance, as the key to an "open, interoperable, secure, and reliable [Internet]." [22].

While such structure implies US unilateral influence may become more diffuse, it reinforces the spirit and character of the Internet.

While the UN and NATO have outlined the initial response frameworks for major cyber attacks, the United States must continue developing and framing adequate prevention measures for the continuous below-response threshold malicious cyber activity that occurs all over the Internet. If network defense and law enforcement mechanisms are not sufficient to mitigate and respond to threats, then the US government will examine cyber, economic, and kinetic options.

The next step involves legislating new mandatory technological, administrative, and personnel standards, as identified in EO 13636, for organizations responsible for critical infrastructure. These entities should:

• formally recognize the NIST Cybersecurity Framework as the defining set of best practices in securing CI/KR;
• participate in the C3VP and ICSJWG;
•undertake DHS-led cybersecurity certification and routine assessment; and
• provide controlled disclosure to DHS of cyber incident forensics.

The federal government should continue to find new and innovative ways to increase sharing of real-time information with critical infrastructure owners while ensuring information classification restrictions do not inhibit the intelligence sharing essential to the cyber safety and resilience.

Threat data must include not only indicators but also the maximum intelligence possible—assuring that it is secure and actionable. Critical infrastructure operators should also have cleared liaison personnel within the NCCIC. That could help eliminate traditional barriers to communication, advocate for rapid declassification of threat intelligence, and ensure that automated information sharing channels like STIX™/TAXII™ are as developed or refined as possible.

DHS should continue developing capabilities to fuse physical and cyber infrastructure situational awareness for a holistic understanding of their interdependencies and potential cascading effects between systems and sectors, for the government and for corporations. DHS should continue to seek and champion ICS and SCADA systems cyber security best practices—such as those developed by ICS-CERT—to provide automatic vulnerability and mitigation recommendations[23] DHS must

also ensure the NIST Cyber security Framework remains as adaptable and dynamic as are the threats to our critical infrastructure. Finally, in the long-term, DHS may consider transitioning the Cyber Security Framework to a nongovernmental entity in the spirit of open and inclusive participation. This might be similar to the gradual shift in Internet governance and oversight from the Department of Commerce to the Internet Corporation for Assigned Names and Numbers (ICANN)[24]. A highly trained and professionalized cyber security corps is the heart of effective cyber security. The DHS should continue to lead and expand cyber security workforce professionalization efforts like NICE. In the same vein, the government should pursue and invest in cyber ranges and simulation exercises. These facilities could promote the integration of DHS, FBI, and DOD experts with ICS and SCADA cyber security staffs to train and exercise skills in a permissive environment with realistic feedback. As General Davis remarked, "[Long-term] institutional capability in cyberspace is about building the right kind of people, including leaders, who truly understand what [cyber] is about, and who can apply the intellectual staying power to secure an advantage for the future."[25].

The federal government must continue to fund and expand the work of the DOE at the National SCADA Test Bed, the leading effort to bring innovation, cyber security, and standards to our critical sectors, which can then be disseminated to private industries. The work conducted within the national labs is the seed corn that will bear true fruit in years to come. From that seed will come key advances in integrated physical and cyber sensor technologies, big data and predictive analytics, trusted supply-chain initiatives, anomalous behavior detection, and secure life-cycle system acquisition and design. However, despite the best layered-security integrating technology with a well-educated workforce, a determined adversary will eventually find an exploitable attack surface and activities must shift from prevention to mitigation.

Conclusions

The topic of the paper, cyber threats to international security, stands out merely by its title as an interesting and challenging area of research. The explanation for it is first and foremost that the area has not yet been sufficiently explored. Due to the intensive development of international relations in cyberspace, conditioned and supported by the speed of the development of technologies and their implementation in the relations of states, organizations and individuals, this area will always be interesting and challenging. That conclusion arises from the constant change of attitudes and technology. It is precisely that instability which indicates that from that specific, interdisciplinary field of research, in 5 or 10 years, it will be possible to draw some new conclusions, and according to them, set some new paradigms and doctrines. Carr states that cyber-warfare has been present for about a decade, but that it is still not well defined. There is no valid international agreement which would establish a legal definition of an act of cyber aggression. In fact, the entire area of international cyber law is still unclear.

The development and availability of information and communications technologies and the ever-present tensions between politically and ideologically different states have conditioned the international relations in cyberspace. Strategic domination in cyberspace has not yet been achieved by any of the entities of international relations. A large number of international entities

demonstrated their presence and willingness to act in cyberspace. That demonstrates a multi polar dimension of cyberspace in which it is very unlikely that domination or bloc division will occur. The reasons lie in the mutual mistrust and fear of espionage in the case of linking the defense systems.
Over the years, we have seen a number of cyber-attacks on SCADA systems. The severity and consequences of attacks vary. Luckily, until now major disasters have mainly been averted. Much of the remaining work is in shaping international consensus on norms of state cyber behavior, enforcing private-sector responsibilities that affect US national interests, and continual investment and effort in refining the interagency leadership in this rapidly changing space. The rise in sophistication and frequency of cyber-attacks, especially against critical sectors, coupled with antiquated and inadequate security practices and the risks from increasing global interconnectivity all demand national unity of effort and international cooperation and consensus to overcome.

REFERENCES

1. Russo-Georgian War, Wikipedia, 2016 en.wikipedia.org/wiki/Russo-Georgian_War.
2. 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', Wired, November 2014 www.wired.com/2014/11/countdown-to-zero-day-stuxnet
3. 'A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever', Wired, January 2015 www.wired.com/2015/01/german-steel-mill-hack-destruction
4. 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', Wired, March 2016. www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid
5. French Coldwell, Chief Evangelist, Metricstream, National Fintech Cybersecurity Summit 2016, Sydney.
6. 2016 Threats Predictions, McAfee Labs, 2016 www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf
7. N. Choucri and D. Goldsmith, "Lost in cyberspace: harnessing the Internet, international relations, and global security," Bulletin of the Atomic Scientists, vol. 68, no. 2, 2012, pp. 70-77.
8. S. Tatalović, A. Grizold, and V. Cvrtila, Suvremene sigurnosne politike. Zagreb: Golden marketing-Tehnička knjiga, 2008.
9. H. Lin, "A virtual necessity: some modest steps toward greater cybersecurity," Bulletin of the Atomic Scientists, vol. 68, no. 5, 2012, pp. 75-87.
10. L. J. Janczewski and A. M. Colarik, Cyber warfare and cyber terrorism. Hershey: Information Science Reference, 2008.
11. Park S, Lee K. Advanced approach to information security management system model for industrial control system. ScientificWorldJournal 2014;2014:348305.
12.Gold S. The SCADA challenge: securing critical infrastructure. Netw Secur 2009;2009(8):18–20.
13. Cardenas A, Amin S, Lin Z, Huang Y, Huang C, Sastry S. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM symposium on information, computer and communications security. ACM; 2011. p. 355–66.
14. Ricker L. Model predictive control of a continuous, nonlinear, two-phase reactor. J Process Control 1993;3(2):109–23. RiskWorld. <http://www.riskworld.net/>. [accessed 16.10.15].

RISI. Industry attacks growing. October 14.
15. Parfomak, Paul. *Pipeline Cybersecurity: Federal Policy*. Congressional Research Service (CRS) R42660. Washington, DC: CRS, 16 August 2012.
16. Tucker, Patrick. "Forget the Sony Hack, this Could Be the Biggest Cyber Attack of 2015." *Defense One*, 19 December 2014. Accessed 8 January 2015. http://www.defenseone.com/technology/2014/12/forget-sony-hackcould-be-he-biggest-cyber-attack-2015/101727/?oref=d-dontmiss.
17. Swearingen, Michael, Steven Brunasso, Joe Weiss, and Dennis Huber. "What You Need to Know (And Don't) About the AURORA Vulnerability." *Power Magazine*, 1 September 2013. Accessed 15 January 2015. http://www. powermag.com/what-you-need-to-know-and-dont-about-the-auroravulnerability/?pagenum=1.
18. Dilanian, Ken. "NSA Director: Yes, China Can Shut Down Our Power Grids." *Business Insider*, November 2014. Accessed 21 November 2014. http://www.businessinsider.com/nsa-director-yes-china-canshut- down-our-power-grids-2014-11?utm_content=bufferbafcd&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.
19. John Boyd, *A Discourse on Winning and Losing* (unpublished set of briefing slides), document mu43947, 1987, Document Collection, Muir S. Fairchild Research Center, Maxwell AFB, AL; and PPD 21, Critical Infrastructure.
20. Tom Dukes, deputy coordinator for cyber issues, Office of the Secretary, Department of State, to the author, e-mail, 8 August 2016.
21. Daniel, J. Michael, Robert Holleyman, and Alex Niejelow. "China's Undermining an Open Internet: We Must Work Together on Reliable Cybersecurity." *Politico*, 4 February 2015. Accessed February 2015. http://www. politico.com/magazine/story/2015/02/china-cybersecurity-14875.html#.VNYJOJ2opcY.
22. Davis, Maj Gen John A., USA. Keynote Address. Armed Forces Communications and Electronics Association International Cyber Symposium. Baltimore, MD: Defense Video and Imagery Distribution System, 2013. http:// www.dvidshub.net/video/294716/mg-davis-afcea#.VD_u0vlbV8E.
23. .ICS-CERT Advisory (ICSA-11-084-01). "Solar Magnetic Storm Impacton Control Systems," 26 March 2011. Accessed 20 April 2015. https://ics-cert.us-cert.gov/advisories/ICSA-11-084-01.
InfraGard website. Accessed 23 October 2014.
24. Hyman, Leonard. "US to Scale Back Its Role in Internet Governance." *TechCrunch*, 19 February 2015. Accessed 24 March 2015. http://techcrunch.com/2015/02/19/1120736/.
25. Davis, Maj Gen John A., USA. Keynote Address. Armed Forces Communicationsand Electronics Association International Cyber Symposium. Baltimore,MD: Defense Video and Imagery Distribution System, 2013. http://www.dvidshub.net/video/294716/mg-davis-afcea#.VD_u0vlbV8E.