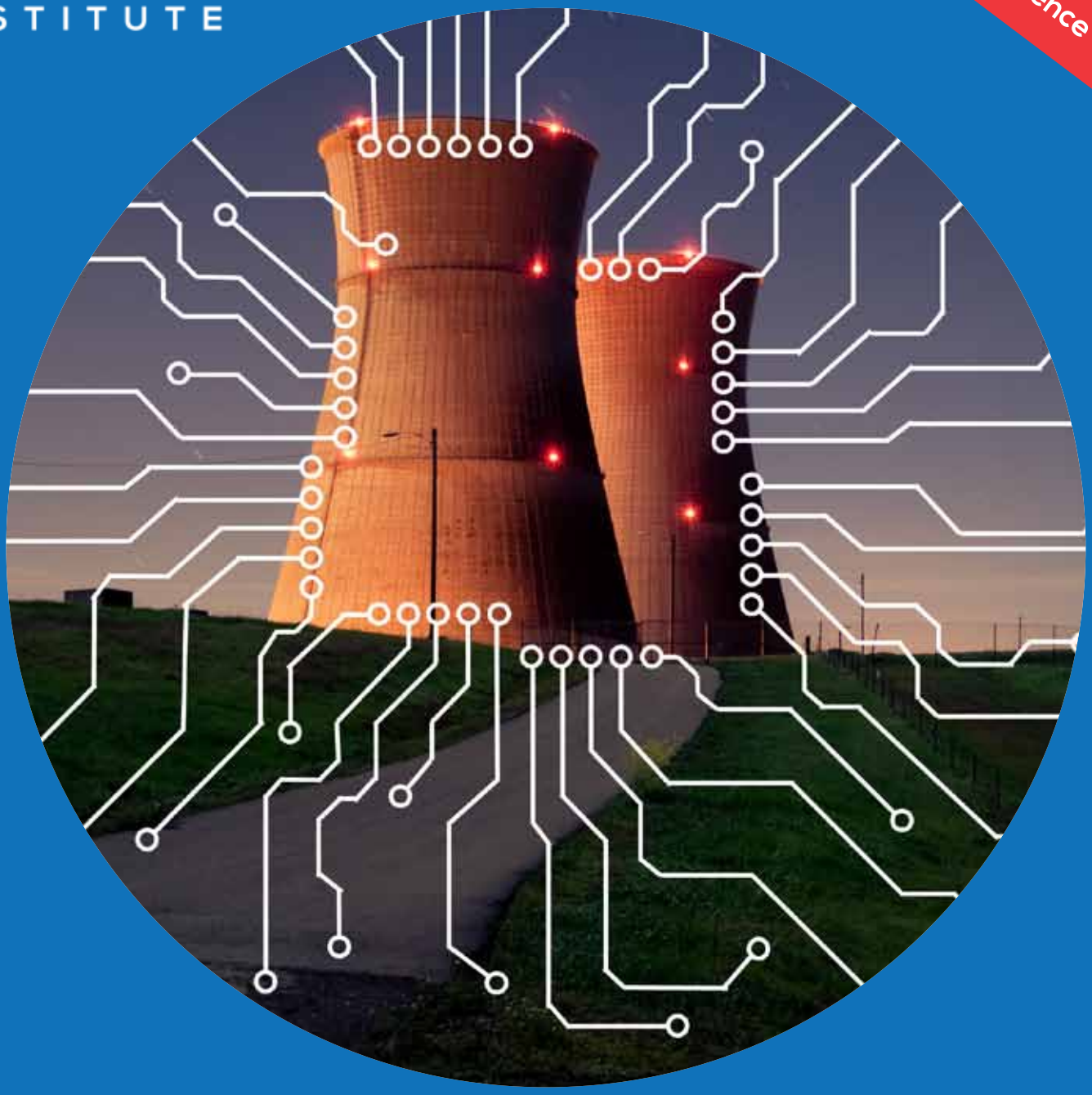
EastWest INSTITUTE

Prepared for the 2014 **Munich Security Conference**



A Measure of Restraint in Cyberspace

Reducing Risk to Civilian Nuclear Assets

POLICY REPORT

1/2014

A Measure of Restraint in Cyberspace

Reducing Risk to Civilian Nuclear Assets

With a preface by **Mohamed ElBaradei**

January 2014

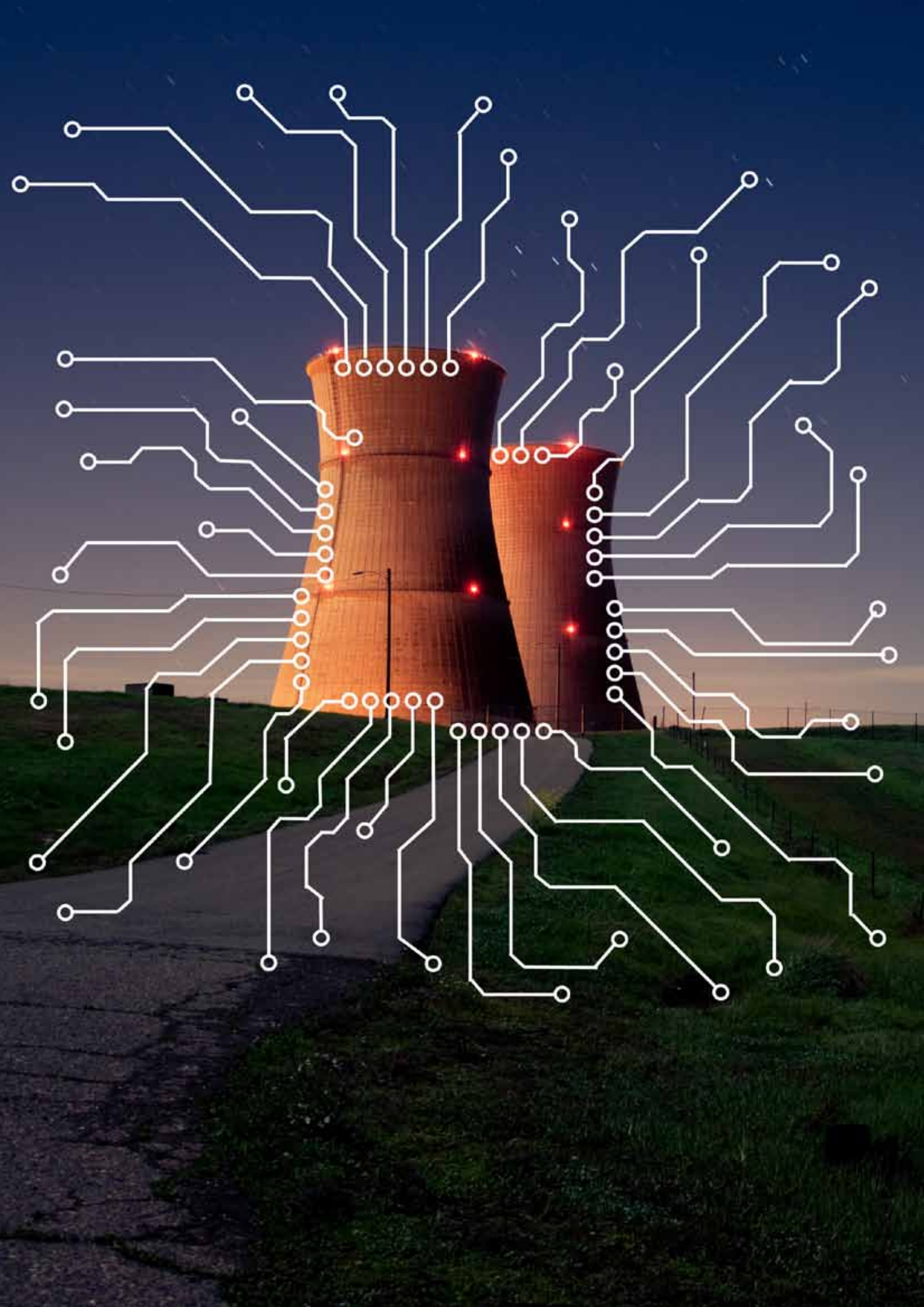


Illustration by Dragan Stojanovski
Photos by T. A. Annis

This discussion paper has been prepared in the framework of the partnership between the EastWest Institute and the Information Security Institute of Moscow State University, which are both members of the International Cybersecurity Consortium.

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a global go-to place for building trust, influencing policies and delivering solutions.

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
+1-212-824-4100

communications@ewi.info
www.ewi.info

PREFACE

Governments and citizens are increasingly aware of and concerned about the potential fragility of civilian nuclear assets in the face of combined natural and man-made occurrences. In this context, I find the growing development and deployment of offensive cyber capabilities by nation-states of concern as a potential threat to the public safety. While experts agree that the probability of a release of radioactive material through a combined physical-cyber attack on such assets is relatively low, the consequences of such a release could be devastating.

In this report, the EastWest Institute takes a refreshingly direct approach, drawing on the successful experiences of global arms control negotiations in non-cyber arenas. The report recommends that states begin to consider a measure of restraint in the uses of cyber weaponry, by foregoing the possibility of using those tools to attack civilian nuclear assets.

I recommend this report to the delegates of the 2014 Nuclear Security Summit in The Hague this March as a continuation of the useful work already underway in that forum.

Mohamed ElBaradei
Former Director General
International Atomic Energy Agency;
Nobel Peace Prize Lauerate

Rancho Seco nuclear power plant
outside Sacramento, California.

FOREWORD

Today, the Internet's unprecedented economic and societal benefits and the vibrancy of global commerce are endangered by three influences: political and economic pressures (including trade protectionism, concerns about domestic stability and anger about surveillance), security concerns (threats to critical infrastructure, cyber-enabled crime and a growing cyber arms race), and the absence of effective national and international cyberspace governance institutions.

In cabinet offices and boardrooms, leaders are asking what can be done to address the cybersecurity "crisis." While this level of interest is overdue, it is important to maintain perspective. Certainly, significant economic damage is done every day by cyber criminals. Yet, serious state-on-state destructive attacks remain countable and measured. The "Stuxnet" attacks in Iran, and the softening up of Georgia's cyber infrastructure prior to a physical invasion remain iconic, not commonplace.

Nevertheless, prudent militaries continue to develop offensive cyber capabilities. Attack via cyberspace is safer and less costly than kinetic attacks. Such capabilities are not inherently bad. They are, however, destabilizing in an environment where there are few rules, where the challenges of attribution could spark misunderstandings, and where an accident could have serious unintended consequences.

Until now, most bilateral work to reduce cyber risk has been focused on confidence building measures, such as hotlines and information sharing about low-level attacks. On a multilateral basis, the United Nations Group of Governmental Experts agreed last year that international law applies in cyberspace, but how it applies remains unclear. A comprehensive approach remains a long way off.

The growth of cyber arsenals and the democratization of access to the technologies of cyber attack mean that time is increasingly short. Rather than wait for comprehensive solutions, the EastWest Institute has focused in this report on a specific next step, adoption of a measure of restraint in the uses of cyber weaponry during peacetime. We propose that nations forego the possibility of using those tools to attack civilian nuclear assets. The report recommends four concrete steps to insulate these peaceful assets from attack while a more comprehensive approach evolves. EWI is also pleased to include an Afterword from our partner organization in Russia, the Information Security Institute of Moscow State University.

The EastWest Institute, through its Global Cooperation in Cyberspace Initiative, will continue to facilitate meaningful progress on the entire range of issues that threaten the future of cyberspace. More information about that initiative can be found at the end of this report.

Bruce W. McConnell
Senior Vice President
EastWest Institute

EXECUTIVE SUMMARY

In 2003, the G8 agreed in broad terms on a common approach to the protection of critical international economic and social assets from cyber attacks. The principles agreed upon have been reiterated in equally broad terms by a number of regional organizations. At the same time, the pressure from the testing and use of offensive cyber weapons by states, the threat of serious terrorist attacks against civilian targets using cyber means, and the demonstrated capabilities of cyber criminals dictate a need to quicken the pace of cooperation. Leading governments have articulated this need but have not succeeded in addressing the wide range of urgent challenges.

This paper proposes specific actions to reduce the cyber risks to civilian nuclear assets, given the grave consequences of possible radiation release in certain circumstances of attack. Although the Stuxnet worm discovered at Iran's Natanz nuclear enrichment facility in 2010 is the most widely-publicized cyber attack against a nuclear facility, the number of less publicized attacks affecting the nuclear sector is constantly increasing. For example, seven attacks inside the United States were reported to the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) during the first half of 2013. This number is merely the tip of the iceberg, as many nuclear operators around the world do not report incidents, fearing the public opinion backlash that can follow, or simply because they are unaware of the attacks.

Despite potentially devastating consequences resulting from cyber attacks on nuclear facilities, progress to advance intergovernmental collaboration to address cyber risks to civil nuclear assets has been slow. In 2012, for instance, the U.S. Department of State research team published a paper, "Cyber Security for Nuclear Power Plants" suggesting that existing UN Conventions be examined in order to identify ways to "extend their provisions to include domestic and international nuclear cyberterrorism."

At a technical level, the International Atomic Energy Agency (IAEA) is working to improve international cooperation in the realm of cybersecurity for nuclear power plants, working closely with the European Network and Information Security Agency (ENISA). These collaborative efforts will be further advanced at the 2015 IAEA Conference on Cyber Security, which will provide an international forum for continued dialogue on how to prevent, detect, and resist emerging cyber threats in the nuclear sector. In addition, governments such as the UK, leading corporations, and organizations like the World Institute for Nuclear Security (WINS) have all been promoting the international sharing of best practice and capability improvements for the protection of critical nuclear information systems and data.

In a parallel infrastructure—civil aviation—important progress has been made. Specifically, at the 2010 Diplomatic Conference on Aviation Security in Beijing, 55 of 76 participating states supported new treaty obligations to forego the use of "technological means," including cyber, to attack

This paper proposes specific actions to reduce the cyber risks to civilian nuclear assets given the grave consequences of possible radiation release in certain circumstances of attack.

civilian aircraft. The United States and China are among 24 countries to have signed the 2010 Beijing Convention and 2010 Beijing Protocol, setting an example for other countries to follow.

The third Nuclear Security Summit, to be held in The Hague in March 2014, provides a key opportunity. At the 2012 summit, 31 states signed the Multinational Statement on Nuclear Information Security that represents a commitment by signatories to share best practices. The Statement emphasizes the importance of working with the IAEA (specifically with its Computer Security at Nuclear Facilities and International Nuclear Security Education Network programs), the International Organization for Standardization (ISO), and the International Telecommunication Union (ITU). The 2014 Summit provides a chance to take this work to the next logical stage, moving beyond confidence building to actual restraint.

This report provides four specific recommendations to strengthen nuclear cybersecurity, as well as encourage broader work on stability in cyberspace. If successful, the measures of restraint advocated here would not only reduce a serious cyber risk, they would demonstrate the ability of nations to make a concrete commitment to temper their activities in cyberspace. Working with the civilian nuclear sector could subsequently help governments and business leaders better determine priorities for the long haul in other sectors.

Recommendations

1. The March 2014 Nuclear Security Summit in The Hague should open a debate among states and corporations with the purpose of promoting early agreement that use of technological attacks (including cyber means) against the safe operation of civil nuclear assets in peacetime should be prohibited by a legally binding multilateral instrument.

2. States should consider the establishment of a multilateral response center for nuclear information security incidents of high severity.

3. States that have not yet signed the 2012 Multilateral Statement on Nuclear Information Security should do so at the 2014 Summit in The Hague and publicize their position.

4. Prior to the 2014 Summit, states that have signed the 2012 Statement should issue and widely publicize an assessment of their performance against the commitments they made, with a view to demonstrating the value of the agreement to non-signatories.

Introduction

More than a dozen states are now pursuing offensive cyber capabilities. This cyberspace militarization drives the urgent need to shield civilian critical infrastructure from peacetime cyber incidents, whether by accident or design.

With broad agreement now secured in the United Nations' Group of Governmental Experts (GGE) on Information Security that the general principles of international law apply in cyberspace,[1] the time is right to begin to operationalize the expected norms of behavior in relation to critical infrastructure (CI) protection. More than a dozen states are now pursuing offensive cyber capabilities. This cyberspace militarization drives the urgent need to shield civilian critical infrastructure from peacetime cyber incidents, whether by accident or design. Among the first of those infrastructures deserving of such consideration is civilian nuclear facilities, where a cyber incident could lead to the release of radioactive material in a densely populated area.

As discussed later, states and infrastructure operators are moving slowly towards international collaboration to help protect CI information assets. This collaboration has been stronger within alliances (such as NATO) and tightly knit groups of states such as the European Union. It has been weaker across big political divides involving major powers, such as Russia, China, the United States, Pakistan, India, Iran and Israel. Teams of international experts however have provided some recommendations that will make this cooperation stronger. Specifically, in 2011, the EastWest Institute (EWI) published a research paper on updating The Hague and Geneva Conventions[2] that encourages creating new agreements for the online environment; the GGE agreement is a step in the right direction. In parallel, the team that produced the Tallinn Manual[3] on the wartime rules for cyberspace has recently published a new study on peacetime rules.[4]

While general agreements are desirable, a practical beginning may be to quarantine selected critical information infrastructure (CII)[5] from cyber attacks during peacetime as a measure of restraint. There is an urgent need to reach consensus, as cyber attacks become more sophisticated and risks to essential services continue to grow.

What Are the Cyber Threats to Civil Nuclear Assets[6]

Civil nuclear assets represent a special case of critical infrastructure given the grave consequences of possible radiation release in certain circumstances of attack.[7]

By 2014, the focus of international concern regarding nuclear information security has expanded to include possible attacks by states. To date, the Stuxnet worm discovered at Iran's Natanz nuclear enrichment facility in 2010 is the most widely-publicized successful cyber attack against a nuclear facility. While there may be debate as to whether Natanz is a "civil" nuclear facility, Stuxnet and its progeny could clearly be used against them. After exploiting several vulnerabilities, the malware attacked the supervisory control and data acquisition (SCADA) systems at Natanz, resulting in the destruction of approximately one thou-

1 UN Docs, A/68/98. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. General Assembly. The United Nations, 24 Jun 2013. Web. 6 Jan 2014. <http://www.mofa.go.jp/files/000016407.pdf>; Psaki, Jen. Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues U.S. Department of State, 7 Jun 2013. Web. 6 Jan 2014. <http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm>.

2 Rauscher, Karl and Andrey Korotkov, "Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace," EastWest Institute, February 2011.

3 *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Edited by Michael Schmitt. Cambridge University Press, 2013. Web. 8 Jan 2014. <http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf>.

4 *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. Edited byKatharina Ziolkowski. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, December 2013. Web. 8 Jan 2014.< http://www.ccdcoe.org/466.html>.

5 CII refers to the information systems, networks and data that support the safe or reliable operation of critical infrastructure.

6 The focus of this paper is civil nuclear assets. This rubric includes radioactive material, nuclear material and civil nuclear facilities (power stations, enrichment facilities, research reactors), systems that transport nuclear fuel or store nuclear waste, and the specialist knowledge or information about these systems. It does not include the supply of electric power from nuclear power stations.

7 Such a release is viewed as a low-probability, but a high-consequence event.

sand centrifuges. According to *The New York Times*, Stuxnet was developed and deployed jointly by the United States and Israel with the apparent objective of slowing down the development of Iran's nuclear program.[8]

But states and terrorists are not the only threats. Industry experts express serious concern about unpredictable consequences caused by system or network attacks, or by using malware. In the first half of fiscal 2013 in the United States, seven attacks that affected the nuclear sector were reported to the Department of Homeland Security's ICS-CERT[9] (even if these were not intended to target exclusively nuclear-related systems).[10] A similar threat level was reported in 2012, when several American nuclear organizations had their enterprise networks compromised. Although ICS-CERT was not aware of any successful breaches of nuclear control networks, exfiltration of data occurred in some of these cases.[11]

Cases of cyber espionage against European and Japanese firms reveal that the threat landscape extends beyond nuclear operators. In 2011, for instance, Mitsubishi Heavy Industries (MHI) was the victim of spear phishing attacks that originated outside MHI's computer network. According to Japan's defense minister, the attacks targeted data on nuclear power plants but did not succeed in accessing important information.[12] Around the same time as this incident, espionage tool Duqu infiltrated computer networks of several European firms that play key roles in nuclear industry; the purpose of the attack was to steal confidential information and reveal vulnerabilities that could be exploited in later attacks.[13]

Press reports show only the tip of the iceberg in terms of existing cyber threats as many nuclear operators around the world do not report incidents, fearing the reputation damage and associated financial backlash that follows perceived cyber vulnerabilities,[14] or simply because they are unaware of the attacks. Even though a complete picture of the complexities and scale of these attacks is missing, the industry, regulatory bodies and many governments have recognized the seriousness of this issue. Specifically, the U.S. intelligence community now regards cyber threat as the top threat to national security.[15] Director of National Intelligence James Clapper opened his March 2013 testimony to Congress by discussing the growing cyber risk facing American CI. He asserted that although it is unlikely for a major attack against CI systems to occur in the next two years, "isolated or non-state actors might deploy less sophisticated cyber attacks as a form of retaliation or provocation."[16]

Industry experts identified at least three specific areas of concern. First, there is the transition that takes place in many existing nuclear plants from analog to digital operating systems. Although this shift is a necessary step in improving long-term safety and performance, it brings with it new cyber vulnerabilities that must be carefully addressed. Some steps have been made in this direction by introducing digital systems on a gradual basis, which helps mitigate the concern and provides operators with more time to adapt to changing security

Civil nuclear assets represent a special case of critical infrastructure given the grave consequences of possible radiation release in certain circumstances of attack.

8 Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times,* 1 Jun 2012. Web. 8 Jan. 2014. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0>.

9 According to its website, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) "works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures." See http://ics-cert.us-cert.gov/.

10 "Brute Force Attacks on Internet-Facing Control Systems," *Incident Response Activity*. ICS_CERT Monitor, Apr 2013, 2. Web. 8 Jan 2014. <http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf>.

11 Goldman, David. "Hacker hits on U.S. power and nuclear targets spiked in 2012." CNN Money, 9 Jan 2013. Web. 8 Jan 2014. <http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/>.

12 "Japan defence firm Mitsubishi Heavy in cyber attack." *Asia-Pacific*. BBC News, 20 Sep 2011. Web. 8 Jan 2014. <http://www.bbc.co.uk/news/world-asia-pacific-14982906>.

13 Williams, Christopher. "Stuxnet-based cyber espionage virus targets European firms." *Telegraph* 19 Oct 2011. Web. 8 Jan. 2014. <http://www.telegraph.co.uk/technology/news/8836633/Stuxnet-based-cyber-espionage-virus-targets-European-firms.html>.

14 Goldman, *supra* n 11.

15 Clapper, James. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, 12 Mar 2013. Web. 8 Jan 2014. <http://www.intelligence.senate.gov/130312/clapper.pdf>.

16 *Ibid.,* 1

demands. Second, the emergence of small modular reactors (SMRs) presents a new security challenge for the industry as data is being collected and stored in a remote centralized data center, making it more vulnerable to intrusion than information that remains entirely quarantined within a single plant. Finally, despite the fact that many experts do not believe in the possibility of radiological material release as a result of a cyber attack,[17] other nuclear industry sources envision a highly coordinated attack combining cyber and physical elements that could increase the likelihood of radiation being released and greatly impact the effectiveness of the security response.

Other nuclear industry sources envision a highly coordinated attack combining cyber and physical elements that could increase the likelihood of radiation being released and greatly impacting the effectiveness of the security response.

Protecting Critical Information Infrastructure (CII)

Increasingly, governments are concerned about protection of CI from cyber attacks. At a broad level though, there are problems in managing differing perceptions of what is "critical."[18] Intrusions on any privately owned infrastructure are unwelcome.[19] And many states and regional organizations simply lack resources to have an impact at the international level.[20] Nevertheless, there has been some progress. In 2003, the G8 Justice and Interior Ministers adopted a broad set of 11 principles that member states are encouraged to consider when developing their national strategies to protect CII. These Principles for Protecting Critical Information Infrastructure are focused on improved warning systems, training programs to personnel from G8 member states and enhanced international cooperation and coordination on the issue.[21] In 2004, the UN General Assembly adopted Resolution 58/199[22] on the "Creation of a global culture of cybersecurity and the protection of critical information infrastructures." An annex to this resolution ("Elements for Protecting CII") is based on the 11 principles articulated by the G8.[23] Moreover, the G8 addresses practical CII issues through its High Tech Crime Sub Group (HTCSG). Established in 1997 and operating as a sub-group of the G8 Roma-Lyon Group (which is designed to combat transnational organized crime and terrorism), the HTCSG has made some important contributions to CII protection. Specifically, it founded the 24/7 Network of Contact Points, an operational network of high-tech experts that assists in performing international cyber investigations and helps address the difficulties of tracing communications on the Internet. The HTCSG's ongoing work to strengthen the 24/7 Network of around 50 states was recognized at the G8 Foreign Ministers meeting in April 2013, where the ministers encouraged these efforts to continue into the future.[24]

The most widely agreed international treaty dedicated to cybersecurity is the Council of Europe's (CoE) Convention on Cybercrime, also known as the Budapest Convention. Parties to the agreement are required to introduce national legislation that criminalizes unauthorised accessing of information and interference with computer data and to provide for extradition to prosecute cyber criminals. It has been signed by 52 states and ratified/acceded by 41. Several of those who have signed or ratified are not member states of the CoE (e.g. United States, Japan and Australia), but uptake is weak outside Western democracies.[25]

Important multilateral work on enhancing CII protection (CIIP) has also been carried out in the European Union (EU). In 2009, for instance, the European Council adopted a Communication on CIIP[26] that led to the adoption of an action plan based on five pillars that reveal a general commitment and a determination to improve structures for

17 *Ibid.*

18 A good recent survey on this issue is Dave Clemente. "Cyber Security and Global Interdependence: What Is Critical?" Web. 8 Jan 2014. Royal Institute of International Affairs, London, 2013. <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf>.

19 *Ibid.*, 34.

20 Portnoy, Michael and Seymour Goodman. "Global Initiatives to Secure Cyberspace: An Emerging Landscape." Springer, Dordrecht NL, 2009, 43.

21 G8 Principles for Protecting Critical Information Infrastructures, Adopted by the G8 Justice & Interior Ministers. May 2003. Web. 8 Jan 2014. <http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf>.

22 A/Res/58/199, adopted 30 January 2004.

23 Brunner, Elgin and Manuel Suter, *International CIIP Handbook 2008/*2009. Swiss Federal Institute of Technology Zurich, 492. Web. 8 Jan 2014. <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf>.

24 G8 Foreign Ministers' Meeting Statement. Web. 8 Jan 2014. <http://iipdigital.usembassy.gov/st/english/texttrans/2013/04/20130411145583.html#axzz2iNtkTjey>.

25 Many states, including Russia and China, have declined calls to sign this convention.

26 "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union," European Commission, Brussels, 07 Feb 2013. Web. 8 Jan 2014. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>.

responses.[27] This communication was set out to coordinate measures to protect Europe from large-scale cyber incidents[28] in response to cyber attacks launched against Estonia in 2007 and Georgia in 2008 and the break of a transcontinental cable in that same year. On June 12, 2012, the European Parliament passed a resolution titled Critical Information Infrastructure Protection: Towards Global Cybersecurity that provides the Commission with specific recommendations for future action in the CIIP field. In 2013, the Commission and the Council issued a draft directive on network and information security to be finalized in 2014.[29] This draft makes clear that the voluntary approach has not provided the necessary results within the Member States, and it requires CI operators, including energy, transport, and "key providers of information society services (e-commerce platforms, social networks), as well as public administrations, to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities."[30] Moreover, it recommends an increase in the capability of national CERTs (Computer Emergency Response Teams). The proposed directive, which will have the force of law in the EU, is more a mobilizer rather than imposer of detailed standards or behaviors apart from the general obligations mentioned earlier.

Another intergovernmental organization that has demonstrated an ongoing commitment to protect critical information infrastructures is the Asia Pacific Economic Cooperation (APEC) group. The APEC Telecommunications and Information Working Group (TEL) was formed in 1990 to improve telecommunications and information infrastructure in the Asia-Pacific region by implementing appropriate policies and cooperation strategies.[31] Relating more directly to CII protection, TEL in 2002 issued its Cyber Security Strategy, which included a "Statement on the Security of Information and Communications Infrastructures". The Strategy encouraged members to work with APEC to develop appropriate laws and policies while closely following the guidelines laid out by the CoE Convention on Cybercrime.[32]

In East Asia, with the Singapore Declaration of 2003, the Association of Southeast Asian Nations (ASEAN) moved to reform its institutional structure to deal with the information security of critical infrastructure for the first time.[33] Other region-wide moves have followed, and individual governments have made strides at the national level.[34] However, transnational cyber threats make the creation of a regional framework and the harmonization of CIIP procedures across national boundaries imperative. Japan and ASEAN have taken a joint lead in advancing the principle of regional cybersecurity cooperation measures for the purposes of CI protection. During the September 2013 Ministerial Policy Meeting on Cyber Security Cooperation, Japan and ASEAN reached a new agreement encouraging senior officials to promote ASEAN's joint efforts in three main areas: 1) to create a secure business environment; 2) to build a secure information and communication network; and 3) to enhance capacity for cybersecurity, including critical infrastructure protection.[35] In addition to such meetings on information security, ASEAN also has a regional forum (ARF) to hold official consultations on peace and security issues. In 2014, the ARF is planning to host a Workshop on Cyber Confidence-Building Measures

Many states and regional organizations simply lack resources to have an impact at the international level.

27 Five pillars include: 1) Preparedness and prevention: to ensure preparedness at all levels; 2) Detection and response: to provide adequate early warning mechanisms; 3) Mitigation and recovery: to reinforce EU defense mechanisms for CII; 4) International cooperation: to promote EU priorities internationally; and 5) Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures. For more information, *see:* "Policy on Critical Information Infrastructure Protection (CIIP)." *Digital Agenda for Europe*. European Commission, 02 Jul 2013. Web. 8 Jan 2014. <http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip>.

28 Downing, Emma. "Cyber Security – A New National Program", UK House of Commons Library, 2011, 17.

29 Impact Assessment: Network and Information Security Directive. Department for Business, Innovation and Skills (BIS). The United Kingdom, 20 Sep 2013. Web. 8 Jan 2014. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/244978/bis-13-1206-network-and-information-security-directive-impact-assessment.pdf>.

30 *Ibid.*

31 Telecommunications and Information. Asia-Pacific Economic Cooperation. Web. 15 Jan 2014. <http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx>.

32 Portnoy and Goodman, *supra* n 20, 48.

33 *See* ASEAN Telecommunications and IT Ministers Meeting (TELMIN). ASEAN Secretariat, 2012. Web. 8 Jan 2014. <http://www.asean.org/communities/asean-economic-community/category/asean-telecommunications-and-it-ministers-meeting-telmin>.

34 Koh, Collin, and Alvin Chew. "Critical Energy Infrastructure Protection: The Case of the Trans-ASEAN Energy Network." *Journal of Energy Security*. (2009). Web. 8 Jan. 2014. <http://www.ensec.org/index.php?option=com_content&view=article&id=205:critical-energy-infrastructure-protection-the-case-of-the-trans-asean-energy-network&catid=98:issuecontent0809&Itemid=349>.

35 Joint Ministerial Statement of the ASEAN-Japan Ministerial policy Meeting on Cybersecurity Cooperation. ASEAN, 13 Sep 2013. Web. 8 Jan 2014. <http://www.asean.org/images/Statement/final_joint_statement asean-japan ministerial policy meeting.pdf>.

In China, in 2012, the Information Security Law Research Center of the Xian Jiaotong University issued a Blue Paper on "China's Protection for Critical Information Infrastructure."

aimed at enhancing transparency in cyberspace and fostering regional cooperation on cybersecurity issues.[36]

Another Asian-based regional intergovernmental organization, the Shanghai Cooperation Organization (SCO), which includes Kazakhstan, China, the Kyrgyz Republic, Russia, Tajikistan and Uzbekistan as members, embraced cybersecurity as an important aspect of its work in 2006.[37] SCO later undertook cooperation with the Black Sea Economic Cooperation (BSEC) with a purpose of protecting information and networks systems in the Black Sea area.[38] Additionally, in 2009, an intergovernmental agreement on cooperation in providing information infrastructure security was reached by SCO member states at the Yekaterinburg Summit. This agreement came into effect in June 2011 after ratification by the six member states.[39] SCO maintains quite high intensity in the diplomacy of information security.

In China, in 2012, the Information Security Law Research Center of the Xian Jiaotong University issued a Blue Paper on "China's Protection for Critical Information Infrastructure."[40] Moreover, during the 67th UN General Assembly, Chinese representative Wu Haitao stressed the need to prevent the information technology arena and outer space from becoming new battlefields. He observed that the threats to information security had become a challenge to the international community; therefore the priority was to formulate global rules to ensure that information technologies were used only for social and economic development.[41] Lastly, on October 20, 2013, a Chinese representative to the United Nations, Liu Ying, made a short statement to the First Committee calling on states to cooperate in the CII protection.[42]

36 "ASEAN Regional Forum - Workshop on Cyber Confidence Building Measures_2014. Concept Paper. Web. 8 Jan 2014. <http://aseanregionalforum.asean.org/files/Archive/20th/ARF%20ISG%20on%20CBMs%20and%20PD,%20Beijing,%2027-28April2013/Annex%2023%20-%20Draft%20Concept%20Paper%20for%20ARF%20Workshop%20on%20Cyber%20Confidence%20Building%20Measures.pdf>.

37 Declaration of the Heads of the SCO Member States on International Information Security, Shanghai, 15Jun 2006. For unofficial translation, *see* http://www.fidh.org/en/Terrorism/Declaration-of-the-Heads-of-the.

38 Muresan, Liviu. "Energy Security-Critical Infrastructures Protection." *In the Perspective of Bucharest NATO Summit 2008.* 15 Jan 2008. Web. 8 Jan 2014. <www.aiprg.net/UserFiles/File/black_sea_conf_papers/.../Liviu_ppt.ppt>.

39 PIR Center Powerpoint, <www.pircenter.org/media/content/files/9/13480961040.ppt>.

40 This document does not give much insight into policy but it is essential reading for anyone working on that China's cyber policies. Above all it demonstrates the relatively recent focus by China on a number of key policy decisions affecting its information security. The document is a useful compendium. The paper is offered as a quick guide, an "introductory note for the international community to understand China's laws, regulations and policies for the protection of critical information infrastructure." The research center describes itself as the "executive body for China's Cloud Computing Security Policy and Law Working Group." It is the organizer for China's Information Security Law Conference and China's Information Security Law Website. The paper identified the following priority sectors: 1) government affairs information systems; 2) Communist Party affairs information systems; 3) livelihood sectors (finance, banking, taxation, customs, auditing, industry, commerce, social welfare, energy, communication and transportation, and national defense industry; 4) educational and governmental research institutes; and 5) public communications, such as radio and television. The composition of the working group which produced the paper is notable, with representatives from the Protection Bureau of the Ministry of Public Security (its Lead Bureau), the First and Third Research Institutes of the Ministry of Public Security, leading private sector corporations (including Microsoft, Intel, Qihoo and Huawei), government and Communist Party agencies, and researchers. For text, *see* http://www.infseclaw.net/UploadFiles/China%E2%80%99s%20Protection%20for%20Critical%20Information%20Infrastructure%20Blue%20Paper.pdf.

41 "Prospects for Nuclear-Weapon-Free World Increasingly Illusive as 'Tectonic Shifts' From Unilateral Measures Affect Strategic Stability, First Committee Told," UN Press Office. General Assembly GA/DIS/3456, 16 Oct 2013. Web. 8 Jan. 2014.<http://www.un.org/News/Press/docs/2012/gadis3456.doc.htm>.

42 Statement by Ms. Liu Ying of the Chinese Delegation at the Thematic Debate on Information and Cyber Security at the First Committee of the 68th Session of the UNGA, 30 October 2013, Web. 8 Jan 2014. <http://www.china-un.org/eng/hyyfy/t1094491.htm>.

The Protection of Nuclear Assets

To date, very few concrete proposals have been made to address cyber risks to civil nuclear assets through new specific multilateral agreements. There are, however, some existing recommendations that warrant brief discussion. In 2012, prior to the Seoul Nuclear Security Summit, the U.S. Department of State research team published a paper, "Cyber Security for Nuclear Power Plants."[43] This paper was meant to prompt government leaders to take specific steps towards improving the cybersecurity of nuclear power plants. It suggested that existing conventions, namely the Convention for the Suppression of Acts of Nuclear Terrorism and the Convention for the Physical Protection of Nuclear Material, be examined in order to identify ways to "extend their provisions to include domestic and international nuclear cyber-terrorism."[44] The research team posited that targeted amendments to specific UN Security Council Resolutions[45] could serve as possible avenues to address nuclear cyber terrorism. They also suggested that the UN Security Council consider classifying certain acts of cyber terror as crimes against humanity. Regrettably, these recommendations do not appear to have received significant attention at the Seoul Summit.

UK-Led Efforts

Following the 2010 Nuclear Security Summit (NSS), the UK has led international efforts to promote and improve nuclear information security with government, industry and academia.[46] The UK government firmly believes that: "Acquiring the material to construct a device is only half the challenge for terrorist groups. Their efforts will fail unless they also acquire the knowledge of how to construct a viable device."[47] Speaking at the 2012 NSS, UK Deputy Prime Minister Nick Clegg declared: "In nuclear issues, information is power and that power in the wrong hands can be used to horrifying effect. That's why the UK has been leading the way on the security of nuclear information."[48] In a news release summarizing Clegg's comments at the 2012 NSS, the British government stated that the information that must be secured "ranges from maps of nuclear sites, [to] how to improvise a device and [to] how to beat border security and emergency response plans."[49]

To advance its efforts, the UK government is working with international organizations, non-governmental organizations and the academic community. More specifically, the Foreign and Commonwealth Office is developing for GICNT partners an online module on Nuclear Information Security, supporting the IAEA in the development of a new nuclear security series document on "Protection and Confidentiality of Sensitive Information in Nuclear Security;" and has assisted the World Institute for Nuclear Security (WINS) in formulating a best practice guide for industry on "Information Security for Operations - Challenges and Opportunities."[50] Within academia, KCL have led work to develop a "Nuclear Information Security Code of Conduct," aimed at raising awareness of the risk posed by the transfer of sensitive nuclear information within the research and academic communities.[51] As part of their wider activity, the UK government has also supported the IAEA in educational and training initiatives to promote nuclear security, including information security. In 2011 King's College London (KCL) launched a two-week international professional development course in nuclear security education aimed at promoting nuclear security culture and information security, through assisting in the development of academic and training courses in this area. Four courses have

To date, very few concrete proposals have been made to address cyber risks to civil nuclear assets through new specific multilateral agreements.

43 Martellini, Maurizio, Thomas Shea, and Sandro Gaycken. "Cyber Security for Nuclear Power Plants," U.S. Department of State, 23 Jan 2013. Web. 8 Jan 2014. <http://www.state.gov/t/isn/183589.htm>.

44 *Ibid.*

45 UN Security Council Resolution, "The Convention on Suppression of Acts of Nuclear Terrorism," S/RES/1540 (2004). Web. 8 Jan 2014. <http://www.un.org/en/sc/1540/>. See also UN Resolution 1373 http://www.un.org/en/sc/ctc/specialmeetings/2012/docs/United%20Nations%20Security%20Council%20Resolution%201373%20(2001).pdf.

46 Pollard, Kane. "The UK Contribution to the 2012 Nuclear Security Summit." PONI Spring Conference. 19 Apr 2012. Web. 8 Jan 2014. <http://csis.org/images/stories/poni/120417_Pollard.pdf>.

47 *Ibid.*

48 "Deputy Prime Minister: information is power in nuclear threat," Deputy Prime Minister's Office, UK, 27 Mar 2012. Web. 8 Jan 2014. <https://www.gov.uk/government/news/deputy-prime-minister-information-is-power-in-nuclear-threat>.

49 *Ibid.*

50 Reding, Anais. "Making information security an integral part of the global nuclear security policy (FCO)." *Civil Service Beta*. UK Government, 14 Oct 2013. Web. 8 Jan 2014. <http://my.civilservice.gov.uk/policy/2013/10/14/developing-nuclear-information-security-policy-through-and-with-others-in-the-foreign-and-commonwealth-office/>.

51 Hobbs, Christopher. "Nuclear Information Security Code of Conduct," Global Partnership Meetings at the Royal Society, UK, 24th October 2013.

The unofficial U.S.-Russia joint policy assessment of October 2013, encourages states to "build on the existing international instruments for warning, interdiction and consequence management of such acts in nation-states."

been held in the UK involving international participants from over 17 countries. As a next step KCL are working in partnership with the University of Witwatersrand in South Africa and other institutes in South East Asia, the Middle East, and North Africa to establish regionally focused professional development courses in nuclear security education.[52]

On November 6, 2013, KCL in partnership with the Royal United Services Institute (RUSI), hosted a high-level workshop on nuclear information security supported by the UK and Dutch governments.[53] Preceding the third Nuclear Security Summit, this workshop—designed to stimulate the discussion on information security among the representatives from government, nuclear industry and academia—covered various topics ranging "the development and application of UK regulations [...to] education/training programmes."[54]

A Russian Proposal

At a 2013 Russia-Netherlands seminar on nuclear information security, a Russian specialist recommended the development of a non-binding international document prohibiting attacks on civil nuclear assets.[55] He also suggested developing a Multilateral Response Centre to serve this purpose. This idea of setting up an emergency response unit in the nuclear information security field is worthy of further review by the international community. Moreover, this proposal addresses the needs identified in the unofficial U.S.-Russia joint policy assessment of October 2013, that encourages states to "build on the existing international instruments for warning, interdiction and consequence management of such acts in nation-states."[56]

IAEA Office of Nuclear Security

The Office of Nuclear Security in the International Atomic Energy Agency (IAEA) operates the Computer and Information Security programme to provide members "with the necessary guidance and external expertise to support the detection of, and response to, criminal or intentional cyber attacks involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities."[57] Its work includes regional training sessions on computer security held several times throughout the year, as well as a number of other courses and conferences for IAEA members aimed at improving the cybersecurity of nuclear power plants.[58] IAEA appears to lead the way internationally in terms of improving cooperation in the realm of cybersecurity for nuclear facilities.[59]

In the Ministerial Declaration of the 2013 IAEA International Conference on Nuclear Security, member states recognized the IAEA's work to improve cybersecurity and encouraged further efforts in this regard, especially in terms of fostering cooperation and providing detailed security guidance to operators. Through its Computer and Information Security program, the agency aims to prevent intrusions that could lead to unauthorized removal of radioactive material, sabotage, and theft of sensitive information. It has produced a series of documents that outline the fundamentals of nuclear cybersecurity, provide technical guidance and offer specific recommendations. Recognizing the evolving nature of the threat and the emergence of new targets such as control and instrumentation systems and mobile computing devices, the IAEA plans to produce additional guidance documents on a rolling basis. Meanwhile, increased demand from member states for advanced training courses on information security and professional development has prompted the IAEA to schedule between six and nine of these courses for 2014. The agency works with other members of the field, as illustrated by its participation in the "@tomic 2012"

52 "Nuclear security education award." King's College London, 18 Sep 2013. Web. 8 Jan 2014. <http://www.kcl.ac.uk/sspp/news/newsrecords/2013/nuclear-education.aspx>.

53 "UK-NL Nuclear Information Security Workshop." 06 Nov 2013. Web. 8 Jan 2014. <http://unitedkingdom.nlembassy.org/agenda/2013/november/uk-nl-nuclear-information-security-workshop.html>.

54 *Ibid.*

55 "The Role of Nuclear Industry in Nuclear Security Governance: Moving to the 2014 Nuclear Security Summit in The Hague." *Russian-Dutch Bilateral Seminar.* 03 Sep 2013. Web. 8 Jan 2014. <http://www.pircenter.org/media/content/files/11/13801355990.pdf>.

56 "Steps to Prevent Nuclear Terrorism: Recommendations Based on the U.S.-Russia Joint Threat Assessment," Belfer Center for Science and International Affairs. Harvard University. Web. 15 Jan 2014. <http://belfercenter.ksg.harvard.edu/files/JTA eng web2.pdf>.

57 Dudenhoeffer, Donald. "Office of Nuclear Security: Cyber Security Programme." Web. 8 Jan 2014. <http://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-21-05-24-TM-NPTD/day-1/5.cybersecurity-dudenhoeffer.pdf>.

58 See http://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf.

59 For examples, *see* https://inlportal.inl.gov/portal/server.pt?open=514&objID=1269&mode=2&featurestory=DA_62265 and http://www.enisa.europa.eu/media/news-items/enisa-cooperating-on-nuclear-cyber-security-with-iaea.

exercise[60] and also the March 2013 meeting with the European Network and Information Security Agency (ENISA) on "Incident Response Planning for Computer Security Events at Nuclear/Radiological Facilities."[61] These collaborative efforts will be further advanced at the 2015 IAEA Conference on Cyber Security, which will provide an international forum for continued dialogue on how to prevent, detect and resist emerging cyber threats in the nuclear sector.

World Institute for Nuclear Security

The World Institute for Nuclear Security[62] (WINS) recently concluded an 18-month governance project aimed at identifying market incentives to promote corporate spending on nuclear cybersecurity. In one workshop, experts from the insurance, legal, cyber and nuclear industries concluded that "despite the many barriers, industry-led self-regulation enhanced by market incentives is necessary to augment existing government regulations, IAEA guidance and international treaties."[63] A number of recommendations generated by the project, some of which will be presented to the Nuclear Industry Summit Working Group on Cyber Security at the 2014 Nuclear Security Summit,[64] focused on the value of creating a cyber design basis threat (DBT) that would promote better definition of the division of responsibilities between governments and nuclear operators. Third party certification of compliance with the DBT would give nuclear operators a direct return on their investment in security.

Despite potential obstacles to the aforementioned proposals, the work of WINS and its partners on this project is currently being validated by initiatives in the United States. U.S. Executive Order 13636 issued in 2013 imposes an obligation on the National Institute of Standards and Technology (NIST) to work with industry to set up a framework for the development of voluntary consensus-based standards and best practices. Notably, both insurance and liability considerations were identified by U.S. Department of Commerce as potential market incentives to foster critical infrastructure cybersecurity.[65]

A Possible Precedent: Civil Aviation

As states continue to debate globally acceptable over-arching approaches to cybersecurity of critical information infrastructure, there has already been important progress in one discrete area—civil aviation. A valuable pledge was made at the 2010 Diplomatic Conference on Aviation Security in Beijing where 55 of 76 participating states supported new treaty commitments (the 2010 Beijing Convention and 2010 Beijing Protocol) to augment existing obligations to prevent the hijacking of aircraft.[66] Among other things, the new commitments oblige signatories to criminalize "technological" attacks on civil air navigation facilities and aircraft in flight. The term "technological attacks" does include cyber attacks. According to the International Civil Aviation Organization (ICAO), the main changes to pre-existing treaties with similar names

As states continue to debate globally acceptable over-arching approaches to cybersecurity of critical information infrastructure, important progress has already been made in one discrete area — civil aviation.

60 "@tomic 2012" was an international table-top exercise focused on the prevention of nuclear terrorism. It included a cybersecurity component and was part of the preparations for the 2014 Nuclear Security Summit.

61 The purpose of the meeting was for the European Union Agency for Network and Information Security (ENISA) "to provide its expertise, and to provide guidance on the process for developing a computer security incident response plan at a nuclear/radiological facility." See http://www.enisa.europa.eu/media/news-items/enisa-cooperating-on-nuclear-cyber-security-with-iaea

62 WINS "provides an international forum for those accountable for nuclear security to share and promote the implementation of best security practices." See https://www.wins.org/index.php?article_id=61.

63 World Institute for Nuclear Security, Corporate Liability and Assurance Mechanisms, WINS Market Incentive Roundtable Report, in partnership with Centre for Science and Security Studies (CSSS), King's College London (KCL) London, United Kingdom, 26 Apr 2013.

64 For an overview of some of the recommendations, see World Institute for Nuclear Security, "Market and Regulatory Incentives for Increased Cyber Security at Nuclear Facilities: The Role of the Design Basis Threat," February 2013.

65 "Discussion of Recommendations to the President on Incentives for Critical Infrastructure Owners and Operations to Join a Voluntary Cybersecurity Program," Web. 8 Jan 2014. <http://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Discussion_Final.pdf>.

66 The text of the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation "was adopted with 55 votes in favour, 14 votes not in favour" and the text of the 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft was adopted "with 57 votes in favour, 13 votes not in favour." See "Final Act of the of the International Conference on Air Law" (Diplomatic Conference on Aviation Security) held under the auspices of the International Civil Aviation Organization at Beijing from 30 August to 10 September 2010, http://www.icao.int/secretariat/legal/Docs/beijing_final_act_multi.pdf. For the text of the Convention, *see* https://www.unodc.org/tldb/en/2010_convention_civil_aviation.html. For the text of the Protocol, *see* https://www.unodc.org/tldb/en/2010_protocol_convention_unlawful_seizure_aircraft.html. For an excellent analysis of the two treaties, *see* http://www.asil.org/insights/volume/15/issue/3/september-11-inspired-aviation-counter-terrorism-convention-and-protocol.

were the criminalization of the acts of using civil aircraft as weapons, using dangerous materials to attack aircraft or other targets, and directing cyber attacks on aircraft in flight.[67] A UN summary of international legal instruments to counter terrorism states that "a cyber attack on air navigation facilities constitutes an offence" under the 2010 Beijing Convention.[68] The United States and China are among 24 countries to have signed the treaties.

Article 6 of the 2010 Protocol limits the effect of the treaty to all situations other than armed conflict. It specifically excludes "The activities of armed forces during an armed conflict, as those terms are understood under international humanitarian law" and "the activities undertaken by military forces of a State in the exercise of their official duties." The latter clause may exclude from the ban those actions currently undertaken by some states in cyberspace against civil aviation, as long as the operation is undertaken by their armed forces. In his 2013 State of the Union address, President Obama alluded to such threats against civil aviation from "enemies" of the United States. [69]

The 2012 Conference on Aviation Security paid considerable attention to capacity building, information sharing and exchange of best practices, with a view to harmonizing national procedures. It also called for standardization of electronic transmission of passenger information and requested ICAO to "further address emerging issues such as air traffic management security (i.e., the security of air navigation services and facilities), landside security, and cyber threats."[70]

Overall, the statement represents a commitment by signatories to share best practices, but avoids addressing issues of criminalization, deterrence, and prevention with regard to attacks against nuclear information security.

The 2014 Nuclear Security Summit: A Key Opportunity

The third Nuclear Security Summit will take place on March 24-25, 2014. It provides an opportunity to build on the work of the previous summit (Seoul 2012) in the area of information security of civil nuclear facilities. During the 2012 summit, 31 states signed the Multinational Statement on Nuclear Information Security[71] based on an initial draft by the UK. There are several positive outcomes of this statement. First, signatories "are now drafting their own legislation to bring in the policies and codes of practice suggested."[72] Second, parties to this agreement have endorsed several general guidelines, one of which is "to enhance cyber security measures concerning nuclear facilities." Third, signatories commit to action on "some or all" of 13 more specific prescriptions targeting national governments, the nuclear industry and the nuclear scientific/academic community and geared towards the implementation of new or improved guidelines, practices and training activities within the domain of nuclear information security. Overall, the statement represents a commitment by signatories to share best practices, but avoids addressing issues of criminalization, deterrence, and prevention with regard to attacks against nuclear information security.

The statement emphasizes the importance of working with the IAEA (specifically with its Computer Security at Nuclear Facilities and International Nuclear Security Education Network programs); the International Organization for Standardisation (ISO); and the International Telecommunication Union (ITU). Additionally, the document highlights UN Security Council Resolutions 1540 and 1887 as key international instruments that should have their information security-related elements implemented by states. However, it does not suggest the amendment of Resolution 1540 to address nuclear cyber terrorism, as suggested by the U.S. Department of State's research report mentioned earlier.[73]

67 ICAO Briefing, "Administrative Package for Ratification of or Accession to the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention, 2010)," Web. 8 Jan 2014. <http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_EN.pdf>.

68 See "United Nations Actions to Counter Terrorism," http://www.un.org/en/terrorism/instruments.shtml.

69 For a discussion of and recommendation to address the ambiguous boundary between war and peace in cyberspace, *see*, Rauscher and Korotkov, "Working Towards Rules for Governing Cyber Conflict," 25, 36-7.

70 Communique of the High-level Conference on Aviation Security (HLCAS) held in Montréal from 12 to 14 September 2012. For text, *see* http://www.icao.int/Meetings/anconf12/IPs/ANConf.12.IP.39.2.1.en.pdf.

71 For text, *see* http://www.whitehouse.gov/the-press-office/2012/03/27/nuclear-security-summit-seoul-march-2012-multinational-statement-nuclear.

72 Reding, *supra* n 50.

73 Martellini, Shea and Gaycken, *supra* n 43.

Conclusions and Recommendations

Some significant progress has been made in the CIIP area. Specifically, the 2012 Multinational Statement on Nuclear Information Security recognized the threat of possible attack on information-technology-based control systems at nuclear facilities. Moreover, there has been notable development around the international sharing of best practice and capability improvements for the protection of critical nuclear information systems and data. Governments such as the UK, leading corporations, the IAEA and WINS have all been playing their part. In the civil nuclear sector however, the pace of international collaboration relative to the potentially catastrophic risk associated with a successful cyber attack is too slow. We make a number of suggestions that may help strengthen international collaboration for nuclear information security, as well as promote broader moves to stability in cyberspace.

Recommendation 1: The March 2014 Nuclear Security Summit in The Hague should open a debate among states and corporations with the purpose of promoting early agreement that use of technological attacks (including cyber means) against the safe operation of civil nuclear facilities in peacetime should be prohibited by a legally binding multilateral instrument.

On the one hand, there are plenty of reasons why states want to retain maximum flexibility for wartime situations in terms of lawful target selection and means of attack. On the other hand, there is a moral and political judgement to be made about humanitarian impacts, even in wartime, of potential release of large amounts of radiation by attacking targets like a nuclear power station.

Recommendation 2: States should consider the establishment of a multilateral response center for nuclear information security incidents of high severity.

This proposal will address a need identified by a team of Russian and American specialists and senior government advisors, as referenced above. It will build on the Russia-United States bilateral agreement to set up an information and communications technology (ICT) incident response mechanism inside their existing nuclear risk reduction center. The most advanced nuclear states may not need such a multilateral mechanism, but less developed states would probably benefit from the existence of a global nuclear industry CERT of some kind.

Recommendation 3: States that have not yet signed the 2012 Multilateral Statement on Nuclear Information Security should do so at the 2014 Summit in The Hague and publicize their new position.

There are some reasonable arguments why the Multinational Statement is not viewed positively by some states. First, it is a relatively weak set of commitments that involve little beyond sharing of best practices and capability development. Second, the administration of civil nuclear assets is not only a domestic sovereign issue but it is also a highly sensitive one. Third, it does little to deter possible attackers. On balance, however, we believe that the statement reflects already stated principles of a number of the leading non-signatories, such as Russia, China and India. These states also stand to benefit from an increase in available means to share best practices and to develop their capacities, and the safety standards of neighboring states with nuclear facilities.

Recommendation 4: Prior to the 2014 Summit, states that have signed the 2012 Statement should issue and widely publicize an assessment of their performance against the commitments they made in it with a view to demonstrating the value of the agreement to non-signatories.

Nuclear information security is a signature security issue of the information age but it has received too little attention. Most states are suffering from an explosion of diplomatic burdens in multilateral diplomacy on issues ranging from climate change to food safety. There has been little room for nuclear information safety to intrude on the busy agendas of many leaders. Even in the framework of the Nuclear Security Summit, it needs to be among the two or three main issues on the table. What justifies an elevation of this issue in wider public debates is the relationship between it and the dilemmas associated with the militarization of cyberspace. Now is the perfect time for states with a commitment to join the UK more visibly in its campaign to advance a common agenda.

We make a number of suggestions that may help strengthen international collaboration for nuclear information security, as well as promote broader moves to stability in cyberspace.

AFTERWORD

Reflections and Supplementary Recommendation on the Subject

With respect to Recommendation 1, using the Beijing precedent as the basis for the criminalization of cyber attacks and joint actions to prevent or prosecute cyber attacks, including through the exchange of intelligence information, we can note that these are in almost complete accord with Russian policy. These attacks are covered by the relevant articles of the Criminal Code of the Russian Federation for the malicious use of software. Russia's law enforcement agencies are working to identify, prevent and eliminate computer-related crime, including in the field of nuclear safety. There is cooperation between the law enforcement agencies of the Russian Federation and the law enforcement agencies of other countries through Interpol. In addition, the signing of the Russian-American agreement on cooperation in the field of international information security in 2013[74] is also a part of Russia's response.

To increase the effectiveness of cooperation in the field of information security for nuclear facilities it would seem appropriate to initiate discussion on the following proposals at the Nuclear Security Summit in The Hague in 2014:

Recommendations for Peacetime

- Identify information and communication systems of nuclear facilities in cyberspace as systems protected under international humanitarian law, and provide an inventory of such systems.
- Consider the benefits of developing a monitoring system, based on national, regional and global capabilities, for violations of international humanitarian law involving the misuse of ICT against nuclear facilities.
- Recognize the misuse of ICT against nuclear facilities as an international crime.
- Assist states that are victims of misuse of ICT against nuclear facilities, including supporting the investigation of the facts in such cases.
- Promote the development of insurance covering breaches of security of nuclear facilities as a result of malicious use of ICT.
- Create additional certification systems for software and hardware intended for use in nuclear facilities.

Recommendations During Hostilities

- Create an inventory of the objects for which military attack by ICTs is prohibited.
- Make perfidy regarding the malicious use of ICT an international crime.
- Provide assistance, international cooperation and participation for neutral states in discovery of evidence of violations of international humanitarian law by malicious use of ICT in the nuclear sphere.

Dr. Anatoly Streltsov
Information Security Institute
Moscow State University

74 Russia-U.S. Joint Statement on Confidence Building Cooperation, 17 June 2013

Предложения по дополнительной теме для координации интересов в области обеспечения информационной безопасности ядерных объектов

Пекинский стандарт, предусматривающий криминализацию кибератак и совместные действия по предотвращению или судебному преследованию кибератак, в том числе, путем обмена разведывательной информацией, во многом был выполнен Российской Федерацией. Уголовный кодекс Российской Федерации включает соответствующие статьи, по которым предусматривается наказание за использование вредоносных программ. Правоохранительные органы работают над выявлением, предупреждением и пресечением компьютерных преступлений, в том числе и в области безопасности ядерных объектов. Налажено сотрудничество правоохранительных структур Российской Федерации с правоохранительными структурами других государств по линии Интерпола. Российская Федерация также подписала российско-американское соглашение (2013г.) по сотрудничеству в области обеспечения международной информационной безопасности.

Для повышения эффективности сотрудничества в области обеспечения информационной безопасности ядерных объектов представляется целесообразным инициировать начало обсуждения следующих вопросов на Саммите по ядерной безопасности в Гааге 2014 г.:

Рекомендации в мирное время

- Идентифицировать информационные и коммуникационные системы ядерных объектов в киберпространстве и составить Реестр таких систем как систем, защищаемых международным гуманитарным правом.
- Рассмотреть возможность и целесообразность разработки системы мониторинга нарушения норм международного гуманитарного права в отношении злонамеренного использования ИКТ против ядерных объектов на базе национальных, региональных и глобальных средств.
- Признать международным преступлением злонамеренное использование ИКТ против ядерных объектов.
- Оказывать помощь государствам – жертвам злонамеренного использования ИКТ против ядерных объектов, в том числе и в области проведения расследования таких фактов.
- Страховать против рисков нарушения безопасности ядерных объектов по фактам злонамеренного использования ИКТ.
- Создать дополнительную систему сертификации программных и технических (аппаратных) средств информатизации, предполагаемых к установке на ядерные объекты.

Рекомендации во время военных действий

- Создать перечень объектов, на которые военные атаки с использованием ИКТ запрещено.
- Признать вероломство в злонамеренном использовании ИКТ международным преступлением.
- Оказывать помощь, обеспечивать международное сотрудничество и участие нейтральных государств в области проведения расследований фактов нарушения норм международного гуманитарного права при злонамеренном использовании ИКТ против объектов ядерной сферы.

Доктор Анатолий Стрельцов
Институт Проблем Информационной Безопасности, Московский Государственный Университет

ACRONYMS

APEC	Asia Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
BSEC	Black Sea Economic Cooperation
CERT	Computer Emergency Response Team
CI	critical infrastructure
CII	critical information infrastructure
CoE	Council of Europe
DBT	design basis threat
ENISA	European Network and Information Security Agency
EWI	EastWest Institute
FCO	Foreign and Commonwealth Office
HTCSG	High Tech Crime Sub Group
GGE	Group of Governmental Experts
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	information and communications technology
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KCL	King's College London
MHI	Mitsubishi Heavy Industries
NSIR	Nuclear Security and Incident Response
NSS	Nuclear Security Summit
SCADA	supervisory control and data acquisition
SCO	Shanghai Cooperation Organization
SMRs	small modular reactors
TEL	Telecommunications and Information Working Group
WINS	World Institute for Nuclear Security

OFFICIAL REFERENCES

A /68/98. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. General Assembly. The United Nations, 24 Jun 2013. Web. 6 Jan 2014. <http://www.mofa.go.jp/files/000016407.pdf>.

Clapper, James. "Statement for the Record." *Worldwide Threat Assessment of the US Intelligence Community*. Senate Select Committee on Intelligence, 12 Mar 2013. Web. 8 Jan 2014. <http://www.intelligence.senate.gov/130312/clapper.pdf>.

"Deputy Prime Minister: information is power in nuclear threat." *The UK is taking decisive action to tackle the threat of nuclear terrorism, Deputy Prime Minister Nick Clegg said today.* Deputy Prime Minister's Office, UK, 27 Mar 2012. Web. 8 Jan 2014. <https://www.gov.uk/government/news/deputy-prime-minister-information-is-power-in-nuclear-threat>.

"Directive 2013/40/EU of the European Parliament and of the Council. "*Official Journal of the European Union*. 8, 12 (Article 1), 14 Aug 2013. Web. 8 Jan 2014. <http://db.eurocrim.org/db/en/doc/1937.pdf>.

G8 Foreign Ministers' Meeting Statement. Web. 8 Jan 2014. <http://iipdigital.usembassy.gov/st/english/texttrans/2013/04/20130411145583.html#axzz2iNtkTjey>.

"G8 Principles for Protecting Critical Information Infrastructures." *Adopted by the G8 Justice & Interior Ministers*. May 2003. Web. 8 Jan 2014. <http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf>.

"Impact Assessment." *Network and Information Security Directive*. Department for Business, Innovation and Skills (BIS). The United Kingdom, 20 Sep 2013. Web. 8 Jan 2014. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/244978/bis-13-1206-network-and-information-security-directive-impact-assessment.pdf>.

"Joint Ministerial Statement of the ASEAN-Japan Ministerial policy Meeting on Cybersecurity Cooperation." ASEAN, 13 Sep 2013. Web. 8 Jan 2014. <http://www.asean.org/images/Statement/final_joint_statement asean-japan ministerial policy meeting.pdf >.

Martellini, Maurizio, Thomas Shea, and Sandro Gaycken. "Cyber Security for Nuclear Power Plants." U.S. Department of State, 23 Jan 2013. Web. 8 Jan 2014. <http://www.state.gov/t/isn/183589.htm>.

Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. Edited byKatharina Ziolkowski. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, December 2013. Web. 8 Jan 2014.<http://www.ccdcoe.org/466.html>.

"Policy on Critical Information Infrastructure Protection (CIIP)." *Digital Agenda for Europe*. European Commission, 02 Jul 2013. Web. 8 Jan 2014. <http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip>.

"Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union," European Commission, Brussels, 07 Feb 2013. Web. 8 Jan 2014.<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>.

Tallinn Manual on the International Law Applicable to Cyber Warfare. Edited by Michael Schmitt. Cambridge University Press, 2013. Web. 8 Jan 2014. <http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf>.

"Prospects for Nuclear-Weapon-Free World Increasingly Illusive as 'Tectonic Shifts' From Unilateral Measures Affect Strategic Stability, First Committee Told," UN Press Office. General Assembly GA/DIS/3456, 16 Oct 2013. Web. 8 Jan. 2014. <http://www.un.org/News/Press/docs/2012/gadis3456.doc.htm>.

Global Cooperation In Cyberspace

"Cyberspace is the future of the human race."

Zhang Li
Director, Chinese Center for Contemporary International Relations

Strategic Objective

To mitigate the negative consequences of global Internet fragmentation, the East-West Institute has launched the Global Cooperation in Cyberspace Initiative.

The Challenge

The Internet's unprecedented economic and societal benefits, and the vibrancy of global electronic commerce, are endangered by government-erected barriers to the flow of information products and services. This development is driven by three influences:

- Political and Economic Concerns: Trade protectionism, concerns about domestic instability, and anger about surveillance create domestic political pressure for "localization."
- Security Concerns: Cyber attackers increasingly menace the delivery of life-sustaining essential services, international cyber criminals go unpunished, and a cyber arms race threatens stability.
- Weak Governance: National and international cyberspace governance institutions are slow, weak, isolated, or non-existent.

If these three influences are not successfully managed, a militarized, fragmented "Splinternet" will emerge to threaten global economic growth and fuel dangerous regional and international instability. Moreover, these interrelated influences cannot be managed separately. Because the network connects everywhere, true cybersecurity will require the participation of all key governments, including many in the developing world. Private sector operators and suppliers, national and international non-governmental organizations, and the netizens themselves must also participate in shaping a common future.

Progress is urgently needed in the near term—every month that passes without action raises the costs to society of the current trends and of turning those trends around. Without effective action, the future safety and livelihoods of literally billions of young, new Internet users will be substantially degraded, increasing pressure on already fragile states.

The Opportunity

The Splinternet is an Internet whose capacity and effectiveness are weakened by barriers to efficient information transfer, threats to personal and public security, and unresolved conflicts around norms. The EastWest Institute will help to create institutions, processes and agreements that will reduce the pressures driving fragmentation and minimize its negative consequences.

The Cooperation in Cyberspace initiative will convene and mobilize government and private stakeholders around three objectives that match the three influences driving fragmentation:

1. Economic Growth: Promote free trade in secure products, encourage the flow of information to promote education and innovation and promote limits on cyber surveillance.
2. Security and Stability: Work to mitigate cyber risks to critical infrastructure, streamline mutual law enforcement assistance in cyber-enabled crime and promote measures of restraint in cyber weapons development and deployment.

3. Sound Governance: Facilitate the design and testing of transparent, accountable, orderly, inclusive and agile management and governance structures that increase predictability and trustworthiness in cyberspace.

The work needed to achieve a secure and stable cyber environment aligns with EWI's mission. The institute takes on seemingly intractable problems that, left unsolved, would result in serious conflict among and within nations on a regional or global scale. Over the past four years, EWI's cyber collaboration has integrated public and private leadership to address several serious challenges in cyberspace. For example, it has worked successfully to catalyze international arrangements to improve communications security, reduce spam, and build bilateral confidence and trust among the U.S., China, Russia and India.

The EastWest Institute has now begun work to achieve the three objectives critical to the continued use of cyberspace and its benefits. These interrelated programs capitalize on its ability to help top corporate and national leaders around the world see the strategic impact of issues. EWI is utilizing its global network of technology/policy experts and senior officials responsible for cyberspace in governments and private organizations. EWI will also use existing partnerships with civil society groups working in this arena and develop new partnerships, so as to maximize effectiveness and efficiency in a resource-constrained environment. It is engaging a diverse set of international companies who provide and use cyberspace to serve their customers. No nation orcompany can solve the problems of cyberspace alone; the same is true for nonprofits, including the EastWest Institute.

The EastWest Institute's senior vice president, Bruce McConnell, a widely-respected cyberspace policy and security leader with over 25 years of experience in public and private sector information policy and technology organizations, is leading this effort. His skills are complemented by existing and new cyber staff and fellows, along with an extensive network of volunteers and partners.

The Work Ahead

The Global Cooperation in Cyberspace Initiative convenes and mobilizes government and private stakeholders around three objectives that will mitigate the impact of the Splinternet: economic growth, security and stability and sound governance. EWI is organizing and facilitating virtual working groups comprised of multi-national public and private sector stakeholders. Two summits (one small and one large) each year will consolidate and showcase results and promote collective action.

Objective: Economic Growth

Influence	Mitigation Approach
Trade protectionism	Promote the benefits of access to secure products and services.
Concerns about domestic instability	Recognize domestic concerns; encourage the flow of information to promote education and innovation.
Anger about surveillance	Internationalize the dialogue about limits.

Objective: Security and Stability

Influence	Mitigation Approach
Threats to the delivery of essential services	Reduce cyber risks to critical infrastructure, e.g., enhance emergency preparedness, and increase confidence in the cyber supply chain.
Cyber-enabled crimes go unpunished	Modernize mutual law enforcement assistance procedures for cyber-enabled crimes.
Cyber arms race threatens stability	Promote measures of restraint, e.g., quarantine civil nuclear facilities, undersea cables, and financial exchanges and clearinghouses from cyber attacks.

Objective: Sound Governance

Existing multi-lateral and multi-stakeholder institutions must be strengthened and their legitimacy enhanced. In some areas, new institutions may be needed. The working groups EWI forms to make progress toward the first two objectives will be "instrumented" to provide lessons about what works in multi-national, multi-sector stakeholder collaboration. For each issue, the institute will create a transparent, accountable, orderly, inclusive, and agile working group. The program will create and test out prototypes of the organizations that are needed to manage global problems in cyberspace and in other domains. This experiential data will be supplemented by research on the strengths and weaknesses of existing international institutions and processes in cyber and other issue domains. The result will be a set of models for institutional design and operation that will serve the effective, long-term governance and management of cyberspace.

About the Authors

Bruce McConnell is responsible for leading EWI's communications and networking with public and private sectors around the world. He also manages the institute's Cooperation in Cyberspace Program, which includes its Worldwide Cybersecurity Initiative. McConnell is also a senior advisor at the Center for Strategic and International Studies. He received a Master of Public Administration from the Evans School for Public Policy at the University of Washington, where he maintains a faculty affiliation, and a Bachelor of Sciences from Stanford University.

Greg Austin leads the institute's Policy Innovation Unit, whose purpose will be to identify and produce a stream of policy papers on new and emerging areas of global risks, threats and challenges. Greg is the author of several highly reviewed books on international security, especially on Asia. In 2003-04, he led a major review for the United Kingdom Cabinet Office on UK conflict prevention policies. He has several post-graduate qualifications in international relations, including a PhD.

Eric Cappon is a recent honors graduate of Queen's University in Canada in the field of political studies. He co-authored this paper as a member of the Policy Innovation Unit at the EastWest Institute.

Nadiya Kostyuk is a Program Coordinator for the EastWest Institute's Worldwide Cybersecurity Initiative. She spent the past two years conducting interviews with government officials, academics and journalists, researching policy gaps in the current European cybersecurity paradigm. In-country experience in Bosnia and Herzegovina, Estonia, Ukraine, Russia, Serbia, Sweden, Switzerland and the Czech Republic provided her with a better understanding of each country's unique political climate.

EastWest Institute Board of Directors

OFFICE OF THE CHAIRMEN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC
Board of Directors
Dell Inc.

Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President, Co-Founder and CEO
EastWest Institute

R. William Ide III (U.S.)
Council and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
McKenna Long and Aldridge LLP

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Former Senior Executive Vice President
Central National-Gottesman Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Tewodros Ashenafi (Ethiopia)
Chairman and CEO
Southwest Energy (HK) Ltd.

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
Chairman and CEO
IP Partners

Robert N. Campbell III (U.S.)
Founder and CEO
Campbell Global Services LLC

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)
Co-founder and Managing Principal
Chertoff Group

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)
Former Foreign Secretary of India

Kevin Taweel (U.S.)
Chairman
Asurion

Amb. Pierre Vimont (France)
Executive Secretary General
European External Action Service
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Mangement, LLC

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.
Co-Founder
EastWest Institute

CHAIRMEN EMERITI

Berthold Beitz* (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor and Minister of Foreign Affairs

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo. Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, OSCE and the UN in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

EastWest Institute Policy Report Series

2013

Afghan Narcotrafficking
A Joint Threat Assessment
Policy Report 2013—1 [EN | RU]

The Path to Zero
Report of the 2013 Nuclear Discussion Forum
Policy Report 2013—2

Threading the Needle
Proposals on U.S. and Chinese Actions
on Arms Sales to Taiwan
Policy Report 2013—3

Measuring the Cybersecurity Problem
Policy Report 2013—4

Frank Communication & Sensible
Cooperation to Stem Harmful Hacking
Policy Report 2013—5 [EN | CH]

2012

Bridging the Fault Lines
Collective Security in Southwest Asia
Policy Report 2012—1

Priority International Communications
Staying Connected in Times of Crisis
Policy Report 2012—2

2011

Working Towards Rules for
Governing Cyber Conflict
Rendering the Geneva and Hague
Conventions in Cyberspace
Policy Report 2011—1 [EN | RU]

Seeking Solutions for Afghanistan, Part 2
Policy Report 2011—2

Critical Terminology Foundations
Russia-U.S. Bilateral on Cybersecurity
Policy Report 2011—3

Enhancing Security in Afghanistan and
Central Asia through Regional
Cooperation on Water
Amu Darya Basin Consultation Report
Policy Report 2011—4

Fighting Spam to Build Trust
China-U.S. Bilateral on Cybersecurity
Policy Report 2011—5 [EN | CH]

Seeking Solutions for Afghanistan, Part 3
Policy Report 2011—6

2010

Economic Development and
Security for Afghanistan
Increasing Jobs and Income with the Help
of the Gulf States
Policy Report 2010—1

Making the Most of Afghanistan's River Basins
Opportunities for Regional Cooperation
Policy Report 2010—2

The Reliability of Global Undersea
Communications Cable Infrastructure
Policy Report 2010—3

Rights and Responsibilities in Cyberspace
Balancing the Need for Security and Liberty
Policy Report 2010—4

Seeking Solutions for Afghanistan, Part 1
Policy Report 2010—5

Building Trust
Delivering Solutions

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a **global go-to place for building trust, influencing policies and delivering solutions.**

–

Learn more at **www.ewi.info**

EastWest INSTITUTE

EWInstitute
EastWestInstitute