APLN
Asia Pacific Leadership Network for Nuclear Non-Proliferation and Disarmament

CNND
Centre for Nuclear Non-Proliferation and Disarmament

Policy Brief No. 17

November 2014

Cyber Threats and Nuclear Dangers

Vincent Boulanin and Tanya Ogilvie-White

Summary

The problem of commercial cyber espionage is insidious, widespread and ever-present, but many other cyber challenges are just as real, and some that currently seem abstract nevertheless need to be taken seriously. The nuclear domain is a case in point: nuclear weapons, materials and facilities are vulnerable to accidents, sabotage or theft, in incidents that can have a cyber dimension. Cyber attacks on nuclear facilities are known to have occurred in the recent past, others could have gone unreported, and numerous scenarios can be envisaged that could have destabilizing or even catastrophic consequences for humankind. This Policy Brief explores cyber threats of varying degrees of probability in the civil and military nuclear spheres: it assesses the measures that are being taken to improve cyber security at nuclear facilities and makes recommendations for next steps to improve the governance of sensitive nuclear information.

Introduction

1. Offensive cyber capabilities pose serious security challenges, especially in the nuclear domain. While the probability of a release of radioactive material through a combined physical and cyber attack on nuclear assets is relatively low, the consequences could be devastating. Awareness of these vulnerabilities is growing, leading states to develop and implement strategies for preventing and managing dangerous cyber incidents. But much more needs to be done. This Policy Brief provides an overview of cyber risks facing civil and military nuclear facilities, examining some of the political and technical questions surrounding cyber incidents. It also assesses the steps that states and international organizations are taking to reduce and manage cyber risks and makes recommendations for improving the governance of sensitive nuclear information.

Cyber Vulnerabilities and Civil Nuclear Facilities

2. The International Atomic Energy Agency (IAEA) has identified three significant risk scenarios involving cyber attacks on civil nuclear facilities:[1]

- A *cyber attack* that corrupts a civil nuclear facility's command and control system, leading to the unauthorized removal of nuclear or another radioactive material. Such an attack would most likely be carried out by a terrorist organization, or by a criminal organization wanting to blackmail a state or company.
- An act of *cyber sabotage*, which affects the normal functioning of a nuclear facility or other parts of the nuclear fuel cycle. States, terrorist organizations, political activists (for example, environmentalist groups) and criminals may all have an interest in this type of furtive cyber operation.
- An act of *cyber espionage*, which results in the collection and exploitation of sensitive nuclear information. This information might be used by a terrorist organization, criminal or state willing

[1] D. Dudenhoeffer, "Office of Nuclear Cyber Security Programme," IAEA, 21 May 2013, http://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-21-05-24-TM-NPTD/day-1/5.cybersecurity-dudenhoeffer.pdf .

to acquire, smuggle or use nuclear material or information for malicious purposes.

3. All three scenarios are feasible, although the first would be very challenging.[2] To obtain material a cyber attack would have to be combined with physical access to remove the material. Most likely physical access would involve an attack on the facility's security forces, which would be risky and difficult (although the level of difficulty would depend on security at the targeted facility, and whether employees there were involved. The latter is known as the "insider threat").

4. It is a different story where the IAEA's second high risk scenario is concerned: there is at least one example of this type of cyber sabotage having taken place, and with some success. The offensive Stuxnet malware, which was revealed in 2010 (and according to David Sanger was developed by the US and Israel[3]) demonstrated that malware could be used to damage civil nuclear facilities via entirely furtive means.[4] Stuxnet was tailor-made to compromise the industrial control system of the Iranian nuclear centrifuges at Natanz, making operators believe that the system was functioning as normal, while in reality, the centrifuges were operating beyond design limits. According to reports, distribution of Stuxnet was achieved via infected flash drives and mobile devices used by contractors who had legitimate access to the Natanz critical system.[5] The attacks did not disable the Iranian nuclear enrichment program, but did in all probability slow it down.[6] So far, no catastrophic damage has resulted from a cyber attack against a nuclear facility, but the Stuxnet attack has demonstrated that new cyber tactics and capabilities are being developed and complacency is not an option.

5. There have also been cases of the IAEA's third scenario: cyber espionage. This is not surprising given that this type of cyber operation does not necessarily have to be technically sophisticated to provide access to sensitive information. A computer virus with a malicious payload, such as a keylogger[7] or spyware[8] installed on the portable device used by a consultant or a researcher, might be sufficient for a cyber-offender to penetrate a trusted network, infect other machines and slowly collect information. An example is the Duqu malware, which affected a research laboratory at Budapest University of Technology and Economics in October 2011. Duqu, which was similar to Stuxnet but used for a different purpose, demonstrated that malware could be used to gain sensitive nuclear-related information without the support of an insider. According to Symantec (a US-based software company that designs secure information systems and publishes annual reports on cyber threats), the designers of Duqu were "looking for information such as design documents that could help them mount a future attack on an industrial control facility."[9]

6. An emerging body of information from non-malicious incidents in the civilian nuclear industry is also instructive when thinking about potential cyber security threats and challenges. Self-replicating malwares that are not originally designed to harm nuclear facilities can unintentionally infect the information systems of nuclear facilities and cause breakdowns. In 2003, a powerful worm called Slammer reportedly infected a nuclear plant in David–Besse, Ohio.[10] The worm infected the high-speed network that a contractor shared directly with the nuclear plant. The malware infected some servers running Microsoft Structured Query Language Server, which had not been updated against that particular worm. The infection paralyzed two important process control systems for several hours. Fortunately, the control system at the

---

[2] EastWest Institute, *A Measure of Restraint in Cyberspace: Reducing Risk to Nuclear Assets*, Policy-Report, January 2014, p. 12.

[3] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Broadway Books, 2012).

[4] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), pp.114–18.

[5] R. Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creator Tried to Achieve* (Arlington: The Langner Group, November 2013), p.11.

[6] I. Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Program," *RUSI Journal* 158: 2 (April 2013): pp. 48–56; D. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times,* 1 June 2012; T. Ricks, "Covert Wars, Waged Virally," *New York Times,* 5 June 2012, http://www.nytimes.com/2012/06/06/books/confront-and-conceal-by-david-sanger.html; Sanger, *Confront and Conceal*.

[7] Keyloggers record key strokes to access confidential data such as passwords and bank details.

[8] Spyware is programmed to copy and leak content.

[9] Symantec, *W32.Duqu: The Precurdor to the Next Stuxnet,* Version 1.4, 23 November 2011, p. 1.

[10] J. Saiz, "Le Ver Slammer s'est Offert une Centrale Nucléaire Américaine," *Security Vibes Magazine,* 5 September 2003.

plant was built on analogue systems, and as a result this breakdown did not lead to significant disruption.

7. However, the event highlighted the need to be aware of cyber security concerns with the progressive transition from analogue to digital control systems in nuclear facilities. With off-the-shelf hardware and software being used in place of tailor-made systems, vulnerability to malware could grow. The multiplication of small modular nuclear reactors could also be problematic, as the data for control systems is no longer quarantined on-site but transferred and stored in remote, centralized data centres.[11]

8. System malfunction or operator errors can also lead to cyber breakdown and affect the normal functioning of nuclear power plants. In 2008, Unit 2 of the Hatch Power plant in Georgia, US automatically shut down after an engineer made a software update to a computer that was used to collect diagnostic data from the process control network.[12] A virus infection could theoretically produce the same kind of breakdown in the process control system as a system malfunction or operator error, and the consequences might be dramatic if the problem is not fixed quickly. Unlike non-nuclear plants, a nuclear power plant cannot be completely shut down overnight. It takes a long time to cool down a nuclear reactor and if the heat produced by the fuel is not properly controlled, the nuclear core can melt down. There have been cases of partial meltdown due to operator errors and systems malfunction in the past – such as the Three Mile Island Unit 2 in the US in 1979.[13] These and other events have led Roger G. Johnston, Head of the Vulnerability Assessment Team, Argonne National Laboratory, to warn that: "the insider threat from careless or complacent employees and contractors exceeds the threat from malicious insiders (though the latter is not negligible). This is partially, though not totally, due to the fact that careless or complacent insiders often unintentionally help nefarious outsiders."[14]

Are Nuclear Weapons also Vulnerable to Cyber Attack?

9. A cyber attack leading to the launch of a nuclear weapon is the ultimate nightmarish scenario, and thankfully the one with the highest barriers to success. The number of actors that would be able to pull off an offensive and complex cyber attack is smaller than commonly assumed. As cyber expert Thomas Rid argues: "vulnerabilities have to be identified before they can be exploited; complex industrial systems need to be understood first; and a sophisticated attack vehicle may be so fine-tuned to one specific target configuration that a generic use may be difficult or impossible."[15] Terrorist groups are unlikely to have the expertise or the resources to pull off such a damaging attack. Even state-sponsored terrorist organizations might not be able to convert financial backing into capabilities on the scale necessary to carry out any complex cyber attack, let alone one involving nuclear weapons.[16]

10. Currently, only militarily powerful states possess sophisticated military cyber capabilities, and few if any would see it as in their interest to launch a major cyber attack on another state in peacetime.[17] The former head of the USCYBERCOM, General Keith Alexander is confident that foreign leaders believe a major cyber attack would be traced back to them, and that such an attack would "elicit a prompt and proportionate response."[18] It is partly for this reason that Eric Gartzke considers complex cyber weapons not as weapons of the weak, but of the strong.

11. Although the probability of a successful cyber attack leading to the launch of a nuclear weapon is extremely low, other scenarios involving military nuclear assets are not as far-

[11] G. Austin, "A Multi-Level-Approach to Nuclear Information Security," Presentation at the Nuclear Knowledge Summit, 21 March 2014.

[12] B. Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10:1 (Spring 2011), p. 21.

[13] Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," p. 19.

[14] Quoted in M. Bunn and S. D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge, MA: American Academy of Arts and Sciences, 2014), p. 18.

[15] T. Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, 35:1 (2012), p. 28.

[16] J. Fritz, *Hacking Nuclear Command and Control*, Paper commissioned by the International Commission on Nuclear Non-Proliferation and Disarmament 2009, icnnd.org/Documents/Jason_Fritz_Hacking_NC2.doc; C. Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress,* CRS Report for Congress, 17 October 2003.

[17] E. Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38:2 (Fall 2013); E. Gartzke, "Cyber-Pearl Harbor is a myth," *Washington Post*, 11 November 2013.

[18] T. Farnworth, "Study Sees Cyber Risk for U.S Arsenal," *Arms Control Association,* April 2013.

fetched. Details are sparse in the public domain, but cyber attacks that might have placed nuclear weapons and related facilities at risk have already taken place. In the early 2000s, attacks on US computer systems used malicious software (known as Trojans) to scan, infiltrate and gather sensitive information from the US Department of Defense, including systems in a US Army Space and Strategic Defense installation, the Naval Oceanic Systems Centre, and Sandia National Laboratories (where much of the US nuclear weapons arsenal is designed).[19] An investigation into the attacks, known as Operation Titan Rain, concluded the attacks emanated from China and were executed and coordinated in a manner that suggested government involvement.[20] The data stolen included classified technical and scientific information about US strategic weapons systems.

12. Similar attacks have occurred in the UK,[21] China, Russia and North Korea. Some attacks were also perpetrated by China, others by Russia and the United States.[22] Others may have taken place elsewhere, and still more could be in the planning stages. If media reports are to be believed, South Korea is currently seeking to develop cyber tools to sabotage Pyongyang's nuclear arsenal,[23] and it is possible that non-state actors are pursuing capabilities to achieve similar goals.

13. As the political and strategic landscape changes, and as cyber capabilities evolve and expand, cyber attacks on military nuclear programs could become a major strategic risk, undermining deterrence credibility, compromising the safety and security of nuclear arsenals, and even leading to conflict escalation and a nuclear exchange. Dismissing this possibility as abstract or fanciful would be unwise, given the occurrence of events that emerge out of the blue, sometimes with horrific consequences. With this in mind, it is helpful to consider some scenarios involving state or non-state cyber attacks on military nuclear assets. Possibilities include developing cyber capabilities:

- To disable the command and control system of a nuclear-armed state, paralyzing its nuclear deterrent (for example, in the context of an inter-state war). This would be extremely difficult to achieve because numerous layers of preventive control are in place, but advanced military powers might be able to develop cyber and other capabilities to undermine these, particularly if they have insider assistance.
- To infiltrate the communication systems of another state to issue false orders, create the impression that the central command has been destroyed, or corrupt early warning systems to create a false alarm. These would also be difficult and complex tasks, and again, insider support would be necessary because these systems are in closed networks.
- To access information about the location of a nuclear weapon. In some nuclear-armed states, the arsenal includes warheads that are delivered by mobile systems. Malicious state or non-state actors could use furtive cyber attacks to access sensitive information on the location and transport schedule of these nuclear warheads to try to steal them.
- To access and exploit information for the design of nuclear explosive devices (either to improve a nuclear explosive device, or to develop radiological weapons). This kind of cyber attack could be launched by a state or a terrorist organization interested in obtaining nuclear weapons or acquiring knowledge that can be exploited in other ways.

14. Of these scenarios, the third and fourth are more feasible, partly because more people are in the loop and therefore more machines are vulnerable to infection: military officials who need to be informed about the location and transport of nuclear warheads, and researchers and technicians involved in the design and maintenance of nuclear weapons. However, even a successful cyber operation along the lines of the third and fourth scenarios would be just one step in a larger plan that could be thwarted at numerous different stages. Should a

[19] P. Shakarian, J. Shakarian and A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Syngress e-books, 2013), pp. 126–27.

[20] F. Gedrich, "A Smackdown Chinese Cyber Thieves Deserve," *Washington Times*, 22 February 2013.

[21] M. Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4:2 (Summer 2011), pp. 7–8.

[22] B. Gellman and E. Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber Operations in 2011, Documents Show," *Washington Post*, 31 August 2013.

[23] Z. Keck, "S. Korea Seeks Cyber Weapons to Target North Korea's Nukes," *The Diplomat*, 21 February 2014, http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/.

terrorist group manage to locate and steal a nuclear weapon, it might not be able to detonate it because most nuclear-armed states use highly sophisticated safety devices whereby the bomb has to be activated by a specific code. There are also mechanisms that prevent detonation and can cause the weapon to self-destruct without explosion if the weapon is exposed to an abnormal environment.[24]

State Responses to Cyber Threats

15. The production, possession and transfer of offensive cyber capabilities cannot be monitored via traditional intelligence activities and arms control regimes.[25] The monitoring techniques that can be applied to tanks, naval vessels and nuclear warheads have no relevance in the cyber realm. Cyber weapons are not countable and states have no interest in revealing their nature. It would be practically impossible to establish an effective oversight mechanism to support an international treaty banning cyber weapons (as suggested by Russia and China in 2011[26]) because no state would allow a third party to scan governmental and military computer systems and networks.

16. This creates a fundamental dilemma: the impossibility of assessing other states' capabilities generates uncertainty and mistrust, which in turn fuels states' haste to improve their cyber military capabilities. If this continues, the world may soon end up with a global "cyber arms race," which will have a detrimental effect on non-proliferation and disarmament and on global security generally. A further deterioration in the level of confidence between states over cyber issues will make the prospects for future multilateral nuclear and conventional disarmament negotiations an even more distant dream.

17. The danger of cyber threats being used to justify backsliding on nuclear disarmament commitments is evident in a report issued by the US Defense Science Board in 2013, which recommended that the US should keep investing in its nuclear arsenal to deter highly destructive cyber attacks on its critical infrastructure by other countries.[27] The report also argued that nuclear retaliation would be justified if a cyber attack had catastrophic consequences for the vital interests of the US and its allies. As critics have pointed out, any change to US nuclear doctrine based on this recommendation would contravene the US obligation to reduce the role of nuclear weapons in its defence and security policies.[28]

18. It is well known that China, Russia and the US are investing heavily in cyber defensive and offensive capabilities and there is a growing mistrust on all sides regarding how these might be used in cyber operations to spy on or undermine each other's nuclear or conventional military capabilities. In an effort to address this problem, the US and Russia announced an agreement on confidence-building in cyber space in June 2013. This includes formal cooperation and information exchange between the US computer emergency response team (CERT) and its Russian counterpart; the creation of a working group on emerging threats; and the use of the existing nuclear hotline to communicate directly during a cyber crisis.[29] The hotline was initially established in 1987 to enable the US and Soviet Union to keep each other informed about missiles tests. Applied to the realm of cyber, the goal is to help prevent misunderstanding and escalation into war between the two countries in the event of serious cyber incidents.[30]

19. However, this agreement appears to be off to a rocky start. Although in November 2013 US and Russian officials held their first working group meeting in Washington to discuss how to implement the June 2013 agreement, in March 2014 a US State Department spokesperson noted that the crisis in Ukraine, and the related deterioration in relations with Russia, might complicate further work on implementation.[31]

---

[24] R. Andersson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Indianapolis: Wiley, 2008), pp. 231–41.

[25] V. Boulanin, "Arms Production Goes Cyber: A Challenge for Arms Control," *SIPRI Essay,* May 2013.

[26] United Nations General Assembly 66th session, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, 14 September 2011.

[27] Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, April 2013).

[28] Remark attributed to B. Blechman, fellow at the Stimson Center. See Farnworth, "Study Sees Cyber Risk for U.S Arsenal."

[29] E. Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security," *Washington Post,* 18 June 2013.

[30] S. Waterman, "Cold War Throwback: U.S.–Russia to Use Nuclear 'Hotline' for New Cyber Showdown," *Washington Post,* 18 June 2013.

[31] "U.S.–Russian Cyber Security Talks Face Uncertainty amid Ukrainian Crisis," *Inside CyberSecurity*, 13 March

At the time the crisis erupted no new dates were agreed for the next round of bilateral cyber security meetings, and at the time of writing, the US government has apparently not agreed internally on when bilateral cyber meetings might resume.

20. A bilateral US–China initiative has not fared much better. In 2013, Washington and Beijing established a cyber security working group in an attempt to build trust and confidence and prevent the further escalation of tensions over mutual cyber espionage activities. The first working group meeting, which was held in July 2013 just before the US–China Strategic and Economic Dialogue, got the initiative off to a good start, and was regarded as a diplomatic coup by US President Barack Obama and China's President Xi Jinping. But in common with the US–Russia cyber initiative, this one is also under severe strain following the US decision to charge five Chinese military officers with hacking into US companies, including Westinghouse Electric (which provides fuel, services, technology, plant design and equipment for the civil nuclear power industry). This has caused a serious diplomatic rift, leading China to suspend its involvement in the cyber working group in May 2014. At the time of writing, the US has said it wishes to discuss a resumption of the group's important work, but it remains unclear whether China shares that enthusiasm.[32]

21. State-led efforts to address cyber threats to civil nuclear facilities have been more productive, although even in the non-military domain many states are reluctant to disclose information about their activities in cyber space, including the steps they are taking to prevent cyber attacks on nuclear facilities and sensitive nuclear information. There are some exceptions, however, and thanks in part to a UK-sponsored initiative, awareness of the need to build trust and confidence through greater transparency in this area is increasingly recognized. A number of states have recently released information on the voluntary measures they are taking to ensure the effective protection of sensitive nuclear information.[33]

22. For example, the United States issued formal regulations in 2009 that require nuclear power plant operators to submit cyber security and implementation schedules. It is also setting up a cyber security directorate at the Nuclear Regulation Commission and is issuing industry regulations to enhance computer security at nuclear facilities.[34] At the 2014 Nuclear Security Summit in The Hague, the United States also announced plans to monitor the activities of US nuclear power plant operators, to track whether they are implementing cyber security regulatory requirements.[35] The cyber security plans of each operator must provide high assurance that information technologies and information control systems will provide adequate protection against cyber attacks.

23. Other countries are following similar paths. Germany has introduced a new regulatory framework dealing with cyber security.[36] Australia included a cyber security component in its national design basis threat and has started to develop detailed guidance for the classification of nuclear security related information. Australia's 2013 International Physical Protection Advisory Service (IPPAS) mission also included a review of arrangements for information security and cyber security at nuclear facilities.[37] Belgium and the Netherlands have taken similar steps and Norway plans to follow suit in 2015.[38] In December 2013, France adopted a law on cyber security and introduced new regulations on the protection and control of nuclear materials, one of which includes a mandatory obligation for operators to report cyber incidents. Canada, the Czech Republic, Hungary and South Korea are in the process of establishing national standards for the protection of electronic data and data systems that align with IAEA guidance and best practice.

2014, http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/us-russian-cybersecurity-talks-face-uncertainty-amid-ukrainian-crisis/menu-id-1089.html.

[32] M. Pennington, "U.S. Seeks Resumption of Cyber Security Group Suspended by China," *Associated Press*, 27 June 2014, http://www.jacksonfree-press.com/news/2014/jun/27/us-seeks-resumption-cyber-talks-china/.

[33] *UK Statement on Nuclear Information Security: Progress Update*, 2014 Nuclear Security Summit.

[34] US Nuclear Regulatory Commission, *Regulatory Guide 5.71; Cyber Security Programs for Nuclear Facilities,* January 2010.

[35] *National Progress Report: United States of America*, 2014 Nuclear Security Summit; M. Holt and A. Andrews, *Nuclear Power Plant Security and Vulnerability* (Washington DC: CRS, 2014), p. 10.

[36] *National Progress Report: Federal Republic of Germany*, 2014 Nuclear Security Summit.

[37] T. Ogilvie-White and D. Santoro, *Preventing Nuclear Terrorism: Australia's Leadership Role* (Canberra: Australian Strategic Policy Institute, January 2014).

[38] *UK Statement on Nuclear Information Security*.

24. Based on the information available in the public domain, the United States and European Union (EU) appear to be at the forefront of efforts to prevent and respond to cyber attacks on nuclear assets and information. The United States and EU member states support their national nuclear operators through information sharing, training activities and technical support for the detection, management and response to cyber incidents through national cyber security agencies, public–private partnerships and CERTs. The European Network and Information Security Agency connects and supports governments and private operators of critical infrastructures (including nuclear operators) with training and information sharing activities, while EU CERT provides support in crisis management. In the United States, the National Cyber Security Division of the Department for Homeland Security supports the security of critical infrastructures against cyber threats. There are also various public–private partnerships dedicated to critical infrastructure protection such as the Critical Infrastructure and Key Resources Cross-Sector Council, which identifies and shares best practices and supports cross-sector strategic coordination and information sharing.

25. The UK and the Netherlands are playing a leadership role in encouraging other states to address cyber vulnerabilities in the nuclear power sector and it is largely thanks to their combined efforts that cyber security was one of the main topics addressed at the 2014 Nuclear Security Summit. The final communiqué of the 2014 summit stressed the need for further cooperation between government, industry and academia on cyber security and encouraged states and the private sector to take effective risk mitigation measures to ensure that systems and network facilities are appropriately secured.[39] However, a survey of national presentations during the summit process suggests that most states remain reluctant to engage constructively on this issue. Moreover, the UK-sponsored Multinational Statement on Nuclear Information Security, which received support from 31 states at the Seoul Summit in 2012,[40] only attracted four additional signatures in 2014 and has not received support from key states such as China, India and Russia.

26. Outside of the summit process, the UK and Netherlands have supported initiatives by the World Institute for Nuclear Security (WINS) and the IAEA on nuclear information security, and have been working with academia to increase knowledge and awareness of cyber vulnerabilities. The British government has been sponsoring work by Kings College London in this area, including funding research on developing a nuclear information security Code of Conduct, and a two-week international professional development course, which attracted participants from 17 states. Kings College hopes to partner with the University of Witwatersrand in South Africa and other institutes in East Asia, the Middle East and North Africa to offer similar professional development courses on a regional basis in future.[41]

27. The Dutch government has also been active: in 2012 it hosted an international table-top exercise known as @tomic 2012, which engaged the IAEA, INTERPOL, UN Interregional Crime and Justice Research Institute and the European Commission in cyber incident prevention and response planning. In 2013, the Dutch Embassy in Moscow, together with the PIR Center, organized a seminar on "The Role of Nuclear Industry in Nuclear Security Governance," during which Russian experts recommended "the development of an international, legally non-binding document or an instrument of soft law prohibiting attacks, authorized by states on objects of nuclear infrastructure."[42]

The Role of International Organizations

28. Beyond the United States, EU member states and a handful of other countries, it is unclear how most countries are addressing cyber threats in the nuclear domain. There is no legal obligation to implement international standards or follow best practice guidelines, and it is likely that some states lack the capacity, political will or security culture that would encourage

[39] "The Hague Nuclear Summit Communiqué," 2014 Nuclear Security Summit, 25 March 2014, http://www.government.nl/documents-and-publications/directives/2014/03/25/the-hague-nuclear-security-summit-communique.html.

[40] Algeria, Australia, Belgium, Canada, Chile, Czech Republic, Finland, France, Georgia, Germany, Hungary, Indonesia, Israel, Italy, Japan, Kazakhstan, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Norway, Philippines, Poland, Republic of Korea, Romania, Spain, Sweden, Switzerland, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States of America and Vietnam.

[41] EastWest Institute, *A Measure of Restraint in Cyberspace*, p. 16.

[42] "The Role of Nuclear Industry in Nuclear Security Governance: Moving to the 2014 Nuclear Security Summit in The Hague," *Russian–Dutch Seminar*, 3 September 2013, http://pircenter.org/media/content/files/11/13801355990.pdf.

them to do so. This has serious nuclear safety and security implications for the states concerned, their immediate neighbours and potentially the world. State-led outreach activities can and do help address this problem, but due to the politically sensitive nature of cyber challenges, which can have a direct impact on national interests, state-led outreach efforts face some resistance.

29. This is one of the reasons international organizations, such as the IAEA and WINS, have such a critical role to play in the cyber domain: they can provide independent, expert advice and capacity-building to government officials and industry representatives who might be less inclined to engage with third-party national authorities or government-sponsored academic programs. This role was emphasized during the IAEA General Conference in September 2013, when the membership highlighted the agency's efforts "to raise awareness of the threat of cyber attacks and their potential impact on nuclear security" and encouraged the Agency to "make further efforts to improve international cooperation and to assist Member States, upon request, in this area by providing training courses and hosting further expert meetings specific to cyber security at nuclear facilities."[43]

30. The IAEA's work in this area is overseen by the Office of Nuclear Security, which runs a cyber security program designed to provide states with the necessary guidance and external expertise to detect and respond to cyber attacks involving nuclear or radioactive material and associated facilities.[44] Available resources include:

- Technical guidance documents, including a reference manual on computer security at nuclear facilities, which was published in 2011.[45] Additional forthcoming publications include an implementation guide on *Information Security, Protection and Confidentiality of Sensitive Information in Nuclear Security* and three technical guides on *Conducting Computer Security Assessment; Computer Security of Nuclear I&C Systems;* and *Computer Incident Response;*
- Technical information exchange forums, including a dedicated cyber security section of the IAEA Nuclear Security Information Portal (known as NUSEC). By June 2012, this had attracted 650 registered users from approximately 70 countries and 16 international institutions;[46]
- Regional training programs, providing courses including basic information and computer security awareness; guidance on conducting cyber security assessments; advanced courses in information and computer security; and professional development courses for nuclear security professionals;[47]
- Expert support for regional and international cyber security exercises, including subject matter expertise for incident response; and
- IPPAS modules on information and computer security.[48]

31. The IAEA also works with other relevant institutions and initiatives. In June 2012, the IAEA and Dutch Forensics Institute signed a partnership agreement to develop best practices including on cyber forensics applied to nuclear security. In March 2013, the Forensics Institute discussed its emerging expertise with the European Network and Information Security Agency on "Incident Response Planning for Computer Security Event at Nuclear/Radiological Facilities." In June 2015, the IAEA will organize a major conference entitled *Nuclear Security in a Computer World: Prevention Detection and Resistance to Emerging Threats*. This conference has the potential to create a new framework for international dialogue on the issue of cyber threats to nuclear security.

---

[43] *Nuclear Security: Resolution adopted on 20 September 2013 during the tenth plenary meeting*, IAEA document GC(57)/RES/10, 10 September 2013.

[44] D. Dudenhoeffer, "Office of Nuclear Security: Cyber Security Programme," IAEA, PowerPoint Presentation, 21 May 2013, p. 2.

[45] *Computer Security at Nuclear Facilities, Technical Guidance, Reference Manual*, IAEA Nuclear Security Series no. 17, 2011.

[46] *Nuclear Security Report 2012*, (GOV/2012(41-GC (56)/15 p. 6.

[47] Between 2007 and 2013, 13 courses were organized: Beijing (Nov. 2011); Bucharest (Sep. 2008); Indonesia (Dec. 2008); Tunisia (May 2009); Lithuania (Aug. 2010); South Korea (Nov. 2010); South Africa (May 2011); Germany (Nov. 2011); Argentina (Dec. 2012); Ghana (Aug. 2013); USA (Aug. 2013); Beijing (Oct. 2013); Jordan (Nov. 2013). Between six and nine courses are scheduled for 2014.

[48] These modules formed part of the most recent IPPAS missions in the Netherlands (2012), Finland (2012), Romania, and Hungary (2013). K. Mrabit, "IAEA Office of Nuclear Security's Initiative in Cyber and Information Security," Presentation at the 57th Regular Session of the IAEA General Conference Senior Regulator Meeting, 19 September 2013, p. 11.

32. WINS also plays a critical role in building cyber security capacity, focusing its efforts on nuclear industry representatives. Since 2011, WINS has organized a series of workshops dedicated to improving information security at nuclear facilities (held in Vienna in April 2011, Toronto in February 2012, and Amsterdam in November 2013). Earlier this year, WINS published an International Best Practice Guide that draws in part on the discussions at the workshops.[49] This guide provides information on how to protect information technology and instrumentation and control systems in a nuclear installation. It notably includes in its appendices tools to benchmark companies' level of computer security. WINS also recently concluded an 18-month project on how market incentives could be used to make companies spend on nuclear cyber security.[50] WINS' work emphasizes the need to create a cyber design basis threat that would help allocate responsibility between nuclear operators and the state.[51] There is evidence that the recommendations of WINS are being examined with a view to developing national implementation systems. For example, the United States is currently exploring a project with the National Institute of Standards and Technology to work with industry to set up a framework for the development of voluntary, consensus-based standards and best practices.[52]

Recommendations

33. Senior management in the nuclear industry needs to be aware of the importance of having a company-wide cyber security strategy that is led from the top. Personnel need to be made aware of cyber risks, introduced to proper 'cyber hygiene' measures and trained to manage cyber incidents. Nuclear facilities need to integrate cyber security concerns at all levels of management. Cyber security needs to be prioritized during transition from analogue to digital process control systems. Special attention has to be given to vulnerabilities emerging from the supply chain because cyber offenders may easily bypass secure systems if they are able to compromise the work of external contractors.

34. Nuclear operators should share information on cyber incidents with relevant authorities and seek the support of the state when relevant. This step might not receive enthusiastic support from the private sector (because many nuclear operators fear reputational loss if they report cyber incidents) but it is a necessary step. Until this happens, it will remain extremely difficult to evaluate threats and map the nuclear industry's progress towards cyber readiness, protection and resilience. France has recognized this and has made the reporting of incidents mandatory.

35. To improve security at nuclear facilities, the division of cyber responsibilities between the public and private sectors needs to be clarified. This could be addressed in ad hoc or more institutionalized national, regional and/or international public–private forums that are specifically dedicated to nuclear cyber security. These forums could regularly organize table top exercises, perhaps using the model of the @tomic 2012 event.

36. In the 2015 session of the UN First Committee, states should sponsor a resolution calling for the development of a legally binding instrument prohibiting cyber attacks against civilian nuclear infrastructure.[53] This could follow the example of the civil aviation security sector. At the 2010 Diplomatic Conference on Aviation Security in Beijing, 55 of 76 participating states agreed on the need to criminalize "technological attacks" (including cyber attacks) on civil air navigation facilities and aircraft in flight in peacetime. This agreement offers an interesting model because it retains flexibility for wartime situations: it does not apply to the activities of armed forces during conflict, as understood under international humanitarian law, or to actions undertaken by the military forces of a state in the exercise of their official duty. However, considering the potential humanitarian impact of radiation release, the agreement

[49] *WINS International Best Practice Guide, Security of IT and IC Systems at Nuclear Facilities*, Group 4 Implementing Security Measures (Vienna: WINS, 2014).

[50] EastWest Institute, *A Measure of Restraint in Cyberspace*, p. 17.

[51] This was the principal recommendation of the Nuclear Industry Summit Working Group on Cyber Security at the 2014 Nuclear Security Summit. Appendix C of the *WINS International Best Practice Guide* provides an example of a generic cyber design basis threat.

[52] EastWest Institute, *A Measure of Restraint in Cyberspace*, p. 17.

[53] See recommendations made by Russian experts at the PIR Center seminar entitled "The Role of Nuclear Industry in Nuclear Security Governance," 3 September 2013, p. 19, http://pircenter.org/media/content/files/11/13801355990.pdf ; see also presentation by G. Austin, "A Multi-Level Approach to Nuclear Information Security," Presentation at the Nuclear Knowledge Summit, 21 March 2014.

could extend to specifically prohibit attacks that might lead to radiation release in wartime.

37. Language on the responsibility of states and industry to improve the security of sensitive nuclear information should be included in any final document and action plan that emerges from the 2015 NPT Review Conference. Switzerland has used the Preparatory Committee of the 2015 NPT Review Conference to highlight cyber vulnerabilities in the nuclear domain and the need to address them. It is in the interests of all states to protect nuclear facilities from cyber threats and consensus language to this effect would help establish an international norm around strong cyber security wherever nuclear and radioactive materials are in use and potentially at risk of sabotage or theft.

38. In the lead up to the 2016 Nuclear Security Summit in Chicago, states, international organizations and NGOs need to shine a bright light on cyber security, including by emphasizing the importance of the Multinational Statement on Nuclear Information Security. We recommend that they:

- Encourage more key states to support the statement, especially China, India and Russia;
- Persuade existing signatory states to demonstrate the value of the statement by reporting more fully on the steps they are taking to improve the security of sensitive nuclear information; and
- Work with the UK to strengthen the statement's content, especially the (currently weak) language on best practices and capability development.[54]

39. States should seriously consider Russia's proposal to set up a multinational response centre for major cyber incidents at nuclear facilities. This would build on the bilateral agreement that the United States and Russia signed in June 2013 (which includes formal cooperation and information exchange between the US CERT and its Russian counterpart), to provide cyber crisis assistance to states with limited resources or competences. Initiatives of this kind could be discussed in regional forums in the lead up to the 2016 Nuclear Security Summit.

40. States should make available a tree of escalatory contacts to facilitate communication between key stakeholders during a cyber incident at a nuclear facility.[55] These contacts could be managed via an IAEA database, which could facilitate interaction between responsible national bodies and experts.

41. States need to provide more financial support to the IAEA to help fund its expanding nuclear security activities, including in the cyber domain. While it is good that IAEA guidance is seen as a sound basis for establishing national information and cyber security policy and programs, more IAEA guidance documents are needed, and these are likely to require regular updating.[56] IAEA in-country assistance activities, such as IPPAS missions and Integrated Nuclear Security Support Plans (INSSPs), are also likely to expand in the years ahead as states grapple with evolving cyber threats. (IPPAS missions include new cyber modules and future INSSPs will include a needs assessment methodology to help improve state and industry responses to cyber incidents that have nuclear safety and security implications).[57]

42. More attention should be given to cyber threats in discussions of nuclear weapons, including debates on the costs and benefits of nuclear retention versus nuclear disarmament. If successful cyber attacks have the potential to corrupt nuclear weapons command and control, at least temporarily, it is also possible that perceptions of cyber threat and vulnerability could undermine deterrence credibility, with unknown consequences. The US Defense Science Board's recommendation to assign a new role for nuclear weapons in response to cyber attack is particularly ill-considered given the increased uncertainty and mistrust associated with evolving cyber capabilities.[58] The risks involved in nuclear weapons possession are growing, which should provide stronger incentives for nuclear-armed states to comply with disarmament obligations, including discussing timelines for deep cuts.

---

[54] EastWest Institute, *A Measure of Restraint in Cyberspace.*

[55] OSCE, 975th Plenary Meeting, Decision no. 1106 on Initial set of OSCE confidence-building measures to reduce the risk of conflict stemming from the use of information and communication technologies, PC Journal No. 975, PC.DEC/1106, 3 December 2013.

[56] *President's Summary*, International Conference on Nuclear Security: Enhancing Global Efforts, 5 July 2013, http://www.iaea.org/newscenter/statements/misc/2013/nspresident050713.pdf.

[57] *Nuclear Security Plan 2014–2017: Report by the Director General*, IAEA document GOV/2013/42-GC(57)/19, 2 August 2013, p. 7.

[58] Defense Science Board, *Task Force Report.*

The Authors

VINCENT BOULANIN is a Researcher with the SIPRI European Security Programme, currently working on cybersecurity and cyber-warfare issues. Previously he was a SIPRI Associated Research Fellow, working with the Arms Production Programme.

TANYA OGILVIE-WHITE is Research Director at the Centre for Nuclear Non-Proliferation and Disarmament. Previously, she was Senior Analyst at the Australian Strategic Policy Institute, Stanton Nuclear Security Fellow at the International Institute for Strategic Studies, London, and Senior Lecturer in International Relations at the University of Canterbury, Christchurch, New Zealand.

APLN and CNND

The **Asia Pacific Leadership Network (APLN)** comprises some forty former senior political, diplomatic, military and other opinion leaders from fourteen countries around the region, including nuclear-weapons possessing states China, India and Pakistan. The objective of the group, convened by former Australian Foreign Minister and President Emeritus of the International Crisis Group Gareth Evans, is to inform and energize public opinion, and especially high-level policy-makers, to take seriously the very real threats posed by nuclear weapons, and do everything possible to achieve a world in which they are contained, diminished and ultimately eliminated. See further http://apln.anu.edu.au.

The **Centre for Nuclear Non-Proliferation and Disarmament (CNND)** contributes to worldwide efforts to minimize the risk of nuclear-weapons use, stop their spread and ultimately achieve their complete elimination. It works in partnership with the Geneva Centre for Security Policy (GCSP) and the Stockholm International Peace Research Institute (SIPRI), and acts as the Secretariat for APLN. The director of the Centre is Professor Ramesh Thakur, former UN Assistant Secretary-General, and it is assisted by a distinguished International Advisory Board chaired by Professor Gareth Evans. See further http://cnnd.anu.edu.au.

APLN/CNND Policy Briefs

These express the views of the authors, and do not necessarily reflect the views of APLN members or the CNND, or other organizations with which the authors may be associated. They are published to encourage debate on topics of policy interest and relevance regarding the existence and role of nuclear weapons.

Funding Support

APLN and CNND gratefully acknowledge the generous support of The Australian National University; the Government of Australia, in particular the Department of Defence and the Department of Foreign Affairs and Trade; the Nuclear Threat Initiative; and The Simons Foundation of Vancouver, Canada.

Contact Us

Centre for Nuclear Non-Proliferation
and Disarmament
Crawford School of Public Policy
The Australian National University
Canberra ACT 0200 AUSTRALIA
Email: cnnd@anu.edu.au
Tel: +61 2 6125 0912; 0466 465 835 (cell)