Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

CMD 15-H8.87A

File / dossier : 6.01.07
Date: 2015-10-08
e-Doc: 4864669

Supplementary Information

Oral presentation

Submission from
A.J. Kehoe

Renseignements supplémentaires

Exposé oral

Mémoire de
A.J. Kehoe

In the Matter of

Ontario Power Generation Inc.

Application to renew the Power Reactor Operating licence for the Darlington Nuclear Generating Station

Commission Public Hearing
Part 2

November 2-5, 2015

À l'égard de

Ontario Power Generation Inc.

Demande concernant le renouvellement du permis d'exploitation pour la centrale nucléaire de Darlington

Audience publique de la Commission
Partie 2

2-5 novembre 2015

Canada

Chatham House Report

Caroline Baylon with Roger Brunt and David Livingstone

Cyber Security at Civil Nuclear Facilities

Understanding the Risks

CHATHAM HOUSE
The Royal Institute of International Affairs

Chatham House Report

Caroline Baylon with Roger Brunt and David Livingstone
September 2015

Cyber Security at Civil Nuclear Facilities

Understanding the Risks

CHATHAM HOUSE
The Royal Institute of International Affairs

Chatham House, the Royal Institute of International Affairs, is an independent policy institute based in London. Our mission is to help build a sustainably secure, prosperous and just world.

The Royal Institute of International Affairs

Chatham House
10 St James's Square
London SW1Y 4LE
T: +44 (0) 20 7957 5700
F: + 44 (0) 20 7957 5710
www.chathamhouse.org

Charity Registration No. 208223

ISBN 978 1 78413 079 4

A catalogue record for this title is available from the British Library.

Cover image © Korea Hydro and Nuclear Power, Handout/Getty Images

Typeset by Soapbox, www.soapbox.co.uk

Printed and bound in Great Britain by Latimer Trend

This publication is printed on recycled paper

Cover image: Workers of Korea Hydro and Nuclear Power Co. participate in an anti-cyber attack exercise at the Wolsong nuclear power plant on 22 December 2014 in Gyeongju, South Korea.

Contents

Foreword

All technologies have their benefits and liabilities. Digital technologies are transforming the way in which people interact with each other and employ machines, and how machines connect to machines. Enormous amounts of data are flowing and being stored; our world increasingly depends on the internet and digitization to be able to function. Vulnerability to theft of these data has become one of the major drawbacks of financial and other commercial transactions. The protection of data and the secure functioning of the critical infrastructure – such as energy, food and water resources, transport and communications – depend on digital technologies functioning safely and securely. Individuals' privacy in regard to, for example, medical records and insurance data is still being breached to detrimental effect. This report, while considering such situations, focuses on a far more dangerous category of cyber attack – when a facility's industrial control systems are disrupted or even captured and harnessed by saboteurs acting either inside or outside the facilities where these systems are located.

Nuclear energy has been seen at different times from differing perspectives as both a blessing and a curse. The concerns about the health risks of ionizing radiation have meant that the nuclear industry has developed a vast array of safety and security measures to prevent the catastrophic release of radiation, and to respond quickly and effectively should such an event occur. However, no technology is immune to accident, misjudgment or deliberate sabotage. The 2011 nuclear disaster at Fukushima Daiichi as a result of the overwhelming Tōhoku earthquake and tsunami is a recent reminder of what can happen when basic prevention protocols and upgrades are not followed through and – perhaps more significantly – when the improbable is recast as impossible and the duty to plan for the overwhelmingly catastrophic is neglected. Yet the role of nuclear power production in the energy portfolio of many countries remains significant and in some regions is growing.

The vulnerability of critical infrastructure has been the subject of some study over recent years, but since the revelation of the digital worm Stuxnet and the impact it is understood to have had on the functioning of the equipment in Iran's nuclear programme, many experts have been concerned that similar attempts to interfere with the physical workings of a nuclear power plant could prove to be a severe risk. Indeed, as this report notes, there have been a number of reported incidents of cyber interference in nuclear power plants and – assuming that the nuclear industry behaves in similar ways to other industries – we ought to assume that these examples represent the visible part of a much more serious problem.

As a result of these concerns, the International Security Department at Chatham House, with the support of the John D. and Catherine T. MacArthur Foundation, undertook to investigate the range of potential risks at the points of intersection between cyber security and nuclear security. A steering group for the project composed of eminent experts in both cyber security and nuclear security was established. Caroline Baylon, Chatham House Research Associate in Science, Technology and Cyber Security, headed the research and analysis on this project, including interviewing 30 industry practitioners. Roger Brunt and David Livingstone, both members of the steering group, also lent their considerable industry expertise to the project and provided valuable contributions to the writing and analysis. The study found that the nuclear industry is beginning – but struggling – to come to grips with this new, insidious threat. The cyber risk to nuclear facilities requires constant evaluation and response, particularly as the industry increases its reliance on digital systems and as cyber criminal activity continues its relentless rise.

It is our intention that the findings of the research and the proposals put forward in this report for dealing with the cyber threat to the civil nuclear energy should be considered in the spirit of assistance and engagement. The nuclear industry is fortunate in having established regulatory systems and international guidance. The Nuclear Security Summit process, with the next meeting due in 2016, and the role of the IAEA in addressing nuclear security and nuclear safety in concert are mechanisms to ensure that this important issue will start to receive more attention. The nuclear industry, regulatory bodies, security establishments, governments and international organizations need to engage with cyber security experts and academics, on a sustainable basis, to formulate robust policy responses through coordinated plans of action to deal with the technical, managerial and cultural shortfalls identified in this report.

Finally, as the report notes in conclusion, many of the findings of this research are applicable to other industries and sectors. Across societies, the wider critical infrastructure – including power grids, transport networks, maritime shipping and space-based communications assets – is similarly vulnerable to cyber attack, with different but potentially equally dire consequences. We hope that this report will speak to those responsible for the safety and security of this critical infrastructure and help to create a culture of pragmatic dialogue between industry and cyber experts, for the common good.

Patricia Lewis
Research Director, International Security
Chatham House

About the Authors

Caroline Baylon is research associate in science, technology and cyber security at Chatham House, where her work has covered topics including critical infrastructure protection, privacy, the digital divide and internet governance. She also serves as editor of the *Journal of Cyber Policy*, Chatham House's peer-reviewed academic journal published by Routledge, Taylor & Francis. She speaks regularly at international conferences and is a frequent media commentator and contributor, most recently writing a series of articles on the challenges that drones pose to nuclear facilities. She is also the author of the Chatham House research paper *Challenges at the Intersection of Cyber Security and Space Security* (2014).

She has been working on cyber security issues since 2003 and most recently served as vice president of the Center for Strategic Decision Research, a think-tank on international security in Paris, where her research focused on cyber crime and cyber warfare. She also worked on behalf of governments and corporations to raise awareness of cyber security challenges, and as a consultant for a number of Silicon Valley startups on business development issues. Early in her career she worked at Stanford University's Center for International Security and Arms Control (CISAC) as a research assistant on nuclear security.

She holds an MSc in social science of the internet from the University of Oxford and a BA in economics from Stanford University.

Roger Brunt was appointed the UK government's regulator for security in the civil nuclear industry as the director of the Office for Civil Nuclear Security, after retiring from the British Army in 2004. He oversaw the introduction of a number of significant security improvements at civil nuclear sites, including the wider deployment of an armed response capability, improved vetting and information security procedures, and measures to test the civil nuclear security regime. He also promoted the merger of the UK's security and safety regulators in 2007 to enhance regulatory coherence in the industry.

Since 2012 he has been a nuclear security consultant specializing in advice on regulatory compliance for governments, regulators and nuclear operators. He is a member of the IAEA director-general's Advisory Group on Nuclear Security, and he contributes to the development of a number of IAEA nuclear security programmes. He is a visiting senior research fellow at King's College London, where he supports professional development courses in nuclear security, and he chairs the World Nuclear Association's Working Group on the Security of the International Nuclear Fuel Cycle.

David Livingstone is an associate fellow at Chatham House, where he has participated in a broad range of projects on national-level risk management, cyber security, counterterrorism, serious organized crime, nuclear security and space security. He has given evidence to the UK parliament, has provided expert witness services to the Central Criminal Court, and is a regular media commentator.

In his previous military career, he was policy lead on Military Aid to the Civil Powers at the UK Ministry of Defence between 1994 and 1999. He was a staff officer in the 'COBR' national crisis management centre, and worked on a number of cabinet official committees dealing with counterterrorism and security. He was a founder member of the cabinet official committee on cyber security in 1996. He currently advises government and commercial clients on security capability development in various capacities, including as cyber security strategy adviser to the Scottish government; doctrine development for the UK Financial Services Virtual Task Force; contributing to National Audit Office studies on the UK's cyber security strategy; and as author of the ACPO (Association of Chief Police Officers) 2011 Cyber Crime Strategy.

Acknowledgments

A large number of people generously lent their expertise to this project.

In particular, we wish to thank the members of the Steering Committee, who gave generously of their time in attending meetings, reading drafts and imparting invaluable advice and wisdom: Irma Arguello, chair of the NPS Global Foundation in Argentina and an associate fellow at Chatham House; Roger Brunt, a nuclear security consultant specializing in advice on regulatory compliance for governments, regulators and nuclear operators; Guido Gluschke, Director of the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences in Germany; David Livingstone, Managing Director of Napier Meridian and an associate fellow at Chatham House; Dr Anita Nilsson, former director of the IAEA Office of Nuclear Security and an associate fellow at Chatham House; Mark Raeburn, CEO of Context Information Services, a provider of independent technical security consultancy services on the prevention of cyber attacks; Dr Tatsujiro Suzuki, former vice chairman of the Japan Atomic Energy Commission and professor at Nagasaki University; and Peter Young, CEO of VEGA Space. Finally, Adrian Freer and Tom Parkhouse of the UK's Office for Nuclear Regulation (ONR) attended meetings and were able to offer helpful advice on the project, but this contribution should not be interpreted as implying that the findings and conclusions of the report constitute the ONR's formal position on dealing with the cyber threat to the civil nuclear sector.

For their important insights, we should like to thank Don Smith, Technology Director, and Tom Finney, Technical Expert, both at Dell SecureWorks; Dale Peterson, CEO of Digital Bond; Mike St John-Green, an independent cyber security consultant formerly of GCHQ and the Office of Cyber Security and Information Assurance in the UK Cabinet Office; Joe Weiss, Managing Partner, Applied Control Solutions (US); Chris Blask, chair of the Industrial Control System Information Sharing and Analysis Center (ICS-ISAC); Andrey Nikishin, Special Projects Director, Future Technologies at Kaspersky Lab; David Grout, Director for Southern Europe, and Raj Samani, Vice President, EMEA and Chief Technology Officer, both at McAfee; Joel Langill, founder of SCADAHacker.com; and Glib Pakharenko of the Ukrainian Information Security Group. For their input we are also grateful to several people at the European Network and Information Security Agency (ENISA): Dr Evangelos Ouzounis, Head of the Resilience and Critical Information Infrastructure Protection Unit; Rossella Mattioli, an expert on ICS-SCADA systems; Dr Konstantinos Moulinos, an expert in network and information security; and Lauri Palkmets, an expert on CERTs; and, in the French Ministry of Ecology, Sustainable Development and Energy, Christophe Quintin, Chief of the Defence and Security Department, and General Christian Riac, Chief of the Department of Nuclear Security. We also thank all of those who contributed their knowledge and experience but do not wish to be identified.

We also wish to thank John Bolger, Cyber Security Officer, Horizon Nuclear Power (UK), and Chris Spirito, International Cyber Lead at The MITRE Corporation, for having read and commented on early drafts of this report.

Thanks also to Dr Robin Niblett, Director of Chatham House, for his feedback and support, and to the International Security Department team at Chatham House for all their hard work in getting this report to publication: Dr Patricia Lewis for reading and commenting on various drafts and for chairing the steering group, and Hannah Bryce, Henry Dodd, Nilza Amaral and Florence Boafo for all their coordination and support.

Particular thanks are due to Margaret May for her skilled editing of this report – her insightful comments have been invaluable in shaping the final text – and to Joanne Maher and all the publications team at Chatham House.

Any remaining errors are our own.

Above all, we are grateful to the John D. and Catherine T. MacArthur Foundation for their generous funding of this project, without which this project would not have been possible.

Acronyms and Abbreviations

BYOD	bring your own device
CERT	Computer Emergency Response Team
CIIP	critical information infrastructure protection
DBT	design basis threat
DDoS	distributed denial of service
EMEA	Europe, Middle East and Africa
ENISA	European Network and Information Security Agency
GPS	global positioning system
HMI	human–machine interface
IAEA	International Atomic Energy Agency
ICS	industrial control system(s)
ICT	information and communications technology
ISIS	Islamic State of Iraq and Syria
IT	information technology
MS-DOS	Microsoft disk operating system
NRC	Nuclear Regulatory Commission
NSA	National Security Agency (US)
OT	operational technology
PLC	programmable logic controller
PWR	pressurized water reactor
R&D	research and development
SCADA	supervisory control and data acquisition
SMEs	small and medium-sized enterprises
SNI	sensitive nuclear information
SPDS	safety parameter display system
TPC	transmission control protocol
VPN	virtual private network

Executive Summary and Recommendations

Recent high-profile cyber attacks, including the deployment of the sophisticated 2010 Stuxnet worm, have raised new concerns about the cyber security vulnerabilities of nuclear facilities. As cyber criminals, states and terrorist groups increase their online activities, the fear of a serious cyber attack is ever present. This is of particular concern because of the risk – even if remote – of a release of ionizing radiation as a result of such an attack. Moreover, even a small-scale cyber security incident at a nuclear facility would be likely to have a disproportionate effect on public opinion and the future of the civil nuclear industry.

Notwithstanding important recent steps taken by the International Atomic Energy Agency (IAEA) to improve cyber security across the sector, the nuclear energy industry currently has less experience in this field than other sectors. This is partly due to the nuclear industry's regulatory requirements, which have meant that digital systems have been adopted later than in other types of critical infrastructure. In addition, the industry's long-standing focus on physical protection and safety has meant that while these aspects of risk response are now relatively robust, less attention has been paid to developing cyber security readiness. As a result, exploiting weaknesses in digital technology could be the most attractive route for those seeking to attack nuclear facilities without fear of interdiction.

The cyber security risk is growing as nuclear facilities become increasingly reliant on digital systems and make increasing use of commercial 'off-the-shelf' software, which offers considerable cost savings but increases vulnerability to hacking attacks. The trend to digitization, when combined with a lack of executive-level awareness of the risks involved, also means that nuclear plant personnel may not realize the full extent of this cyber vulnerability and are thus inadequately prepared to deal with potential attacks. There is a pervading myth that nuclear facilities are 'air gapped' – or completely isolated from the public internet – and that this protects them from cyber attack. Yet not only can air gaps be breached with nothing more than a flash drive (as in the case of Stuxnet), but the commercial benefits of internet connectivity mean that nuclear facilities may now have virtual private networks and other connections installed, sometimes undocumented or forgotten by contractors and other legitimate third-party operators.

Meanwhile, hacking is becoming ever easier to conduct, and more widespread: automatic cyber attack packages targeted at known and discovered vulnerabilities are widely available for purchase; advanced techniques used by Stuxnet are now known and being copied; and search engines can readily identify critical infrastructure components that are connected to the internet.

In the light of these concerns, Chatham House undertook an 18-month project in 2014–15 on the nexus between cyber security and nuclear security. By drawing on in-depth interviews with 30 industry practitioners, as well as policy-makers and academics, and convening three expert roundtables, the project sought to assess the major cyber security challenges facing the wider nuclear industry; to identify international policy measures that could help to enhance cyber security in the sector; and to help increase knowledge of current concerns in this area. This report examines the major cyber threats to civil nuclear facilities, focusing in particular on those that could have an impact on industrial control systems, and suggests some potential solutions to these challenges.

Main findings

The research identified the following major challenges for civil nuclear facilities.

Industry-wide challenges

- The **infrequency of cyber security incident disclosure** at nuclear facilities makes it difficult to assess the true extent of the problem and may lead nuclear industry personnel to believe that there are few incidents. Moreover, **limited collaboration with other industries or information-sharing** means that the nuclear industry tends not to learn from other industries that are more advanced in this field.
- A **paucity of regulatory standards,** as well as limited communication between cyber security companies and vendors, are also of concern.
- This suggests that **the industry's risk assessment may be inadequate;** as a consequence, there is often **insufficient spending on cyber security.**
- **Developing countries may be particularly at risk,** because they have even fewer resources available to invest in cyber security.

Cultural challenges

- **Nuclear plant personnel, who are operational technology engineers, and cyber security personnel, who are information technology engineers, frequently have difficulty communicating,** which can lead to friction. In many cases the problem is exacerbated by the off-site location of cyber security personnel.
- **Nuclear plant personnel often lack an understanding of key cyber security procedures,**

finding that the procedures documents produced by cyber security personnel do not communicate this information in language that is clear to them.

- **Cyber security training at nuclear facilities is often insufficient.** In particular, there is a **lack of integrated cyber security drills** between nuclear plant personnel and cyber security personnel.
- **Reactive rather than proactive approaches to cyber security** contribute to the possibility that a nuclear facility might not know of a cyber attack until it is already substantially under way.
- This suggests that **nuclear plants may lack preparedness for a large-scale cyber security emergency,** particularly if one were to occur **outside normal working hours.**

Technical challenges

- **Many industrial control systems are 'insecure by design',** since cyber security measures were not designed in from the beginning.
- **Standard IT solutions such as patching are difficult to implement** at nuclear facilities, mainly owing to concern that patches could break a system and because of the commercial need to reduce plant downtime.
- **Supply chain vulnerabilities** mean that equipment used at a nuclear facility risks compromise at any stage.

Recommendations

The cyber security threat requires an organizational response by the civil nuclear sector, which includes, by necessity, knowledgeable leadership at the highest levels, and dynamic contributions by management, staff and the wider community of stakeholders, including members of the security and safety communities. The nuclear sector as a whole, taking account of recommendations and guidance issued by the IAEA, should take a strategic approach that will:

- **Develop a more robust ambition** to match or overtake its opponents in cyberspace and thereby take the initiative, focusing its resources on critical elements of the nuclear fuel cycle.
- **Fund the promotion and fostering of cyber security** within the industry, aiming to encourage a sectoral-level approach, from the highest levels down to the individual.
- **Establish an international cyber security risk management strategy** designed to maintain momentum and agility, incorporating the necessary mechanisms for in-depth preparation to meet cyber security challenges, however these may arise, and a flexible and coordinated response.
- **Develop coordinated plans of action to address the technical shortfalls** identified, such as in patch management, and make the necessary investments.
- **Include all stakeholders** in the organizational response. This will require knowledgeable leadership at the highest levels, the free flow of information and dynamic contributions by management, staff and the wider community of stakeholders, including members of the security and safety communities.
- **Promote an environment that enables the appropriate balance between regulated and self-determined actions** to avoid any tendency for overall stagnation.

Specific recommendations

The report proposes a number of specific recommendations to address the challenges identified.

Assessing the risk – and attracting investment

- **Develop guidelines to measure cyber security risk in the nuclear industry,** including an integrated risk assessment that takes both security and safety measures into account. This will help improve understanding of the risk among CEOs and company boards and make cyber security in the nuclear sector more commercially attractive.
- **Promote cyber insurance,** which will require strong risk assessments, as an effective way to drive the process of implementing change.

Handling the 'human factor'

- **Engage in robust dialogue with engineers and contractors to raise awareness of the cyber security risk,** including the dangers of setting up unauthorized internet connections.
- **Establish rules where these are not already in place** – such as banning personal devices from control rooms and requiring nuclear plant personnel to change the default passwords on equipment – and enforce these rules through a combination of independent verification methods and technical measures, for example by blocking off USB ports.

Promoting disclosure and information-sharing

- **Encourage nuclear facilities to share threat information anonymously** (such as by revealing 'indicators of compromise') in order to promote greater disclosure, since the reluctance to disclose cyber attacks stems partly from concerns for damage to reputation.
- **Promote industry conferences and other measures to enhance interpersonal relationships** in order to encourage informal sharing initiatives, even if governments are dissuaded by national security concerns from sharing threat information at the international level.
- **Governments should lead the establishment of national Computer Emergency Response Teams (CERTs) specialized in industrial control systems,** particularly since they recognize that information-sharing at a national level is key.
- **The regulator should reassure owner-operators** that they will not be penalized for any information that they share, provided they show good faith.

Developing further international policy measures

- **Encourage all countries that have not yet done so to adopt an effective regulatory approach to cyber security at nuclear facilities.** Since a large number of countries follow IAEA guidance, allocating more resources to the IAEA to enable it to develop recommendations on responding to cyber security threats could generate significant benefit.
- **Provide technical and funding assistance to developing countries** in order to improve cyber security at their nuclear facilities.

Bridging communication gaps – including the need for cultural change

- **Establish integrated projects between nuclear plant personnel and cyber security personnel,** such as the preparation of cyber security training materials and undertaking of joint vulnerability analyses. This would also encourage IT personnel to visit the nuclear facility in person on a regular basis to aid mutual understanding.
- **Improve the frequency and quality of cyber security training at nuclear facilities,** potentially involving accreditation of training programmes by the IAEA, **and hold integrated scenario-led drills** between nuclear plant personnel and cyber security personnel to hone skills and develop common understandings and practices.
- **Promote the further creation of more cross-disciplinary university programmes** aimed at training cyber security specialists in the nuclear industry.
- **Foster partnerships between vendors and cyber security companies** to enable the development of more robust cyber security products.

Enhancing security – including the need for 'security by design'

- **Promote the importance of 'security by design',** so that future generations of industrial control systems incorporate security measures during the initial conception phase. This may mean **avoiding superfluous digital features** as well as **incorporating authentication and encryption technologies.**
- **Ensure that sufficient redundancy is retained** in digitlized systems.
- **Promote the use of 'whitelisting',** which restricts the unprecedented flexibility of digitized industrial control systems and also reduces the need to patch systems.
- **Implement intrusion detection systems such as network monitoring** of traffic for anomalous behaviour across the entire control system network, not just on the network perimeter.
- **Encourage the further adoption of secure optical data diodes.**
- **Ensure the integrity of the supply chain.**
- **Prioritize key areas for cyber security investment,** including identifying critical cyber assets at each nuclear facility.

1. Introduction

Recent high-profile cyber attacks on nuclear facilities have raised new concerns about their cyber security vulnerabilities. This is of particular import because of the potential – even if remote – for the release of ionizing radiation as a result of a cyber attack. Given the sensitivities surrounding the nuclear industry, even a small-scale cyber security incident at a nuclear facility would be likely to have a disproportionate effect on public opinion and the future of the industry itself.

Meanwhile, cyber criminal activity is becoming ever easier to conduct, and more widespread: automatic cyber attack packages targeted at known and discovered vulnerabilities are widely available for purchase, and search engines can readily identify nuclear facilities and other critical infrastructure that are connected to the internet. As states and terrorist groups expand their online activities, the fear of a serious cyber attack is ever present as well.

At the same time, nuclear facilities are increasingly making use of digital systems, commercial off-the-shelf software and internet connectivity – all of which provide efficiency and cost-saving benefits but also make facilities more susceptible to cyber attack. As these changes are currently under way, personnel at nuclear facilities may not realize the full extent of their cyber vulnerability. Some still cling to the myth that nuclear facilities are 'air gapped' – or completely isolated from the public internet – and that this protects them from cyber attack. Yet not only can air gaps be breached with nothing more than a flash drive but a number of nuclear facilities have virtual private networks (VPN) or undocumented or forgotten connections, some installed by contractors.

The nuclear industry as a whole is currently struggling to adapt to these changes. Notwithstanding important recent steps taken by the International Atomic Energy Agency (IAEA), the industry's long-standing focus on safety and physical protection has meant that while these systems are now relatively robust, less attention has been paid to upgrading cyber security. In addition, its relatively late adoption of digital technologies means that it has less experience than other sectors in this area. As a result, exploiting weaknesses in digital technology may be a particularly attractive route for those seeking to attack nuclear facilities.

Other characteristics of the sector, such as the associated national security sensitivities, make disclosure of cyber security incidents that have occurred less likely, leading nuclear industry personnel to believe that cyber attacks are less of a threat than is actually the case. It also means that the sector's limited collaboration with others leaves it unable to learn from those with greater cyber security readiness. Furthermore, the rapid evolution of the threat means that regulatory standards are currently inadequate. As a result there is insufficient spending on cyber security, including a lack of funding for agencies poised to deal with the challenge.

All this suggests that the industry's threat assessment or risk calculation may be inappropriate, and that it is not investing as much as it should in cyber security. Consequently the cost–security equation may be out of balance. Developing countries may be particularly at risk, because they have even fewer resources available.

There are also significant issues in the culture of the industry that contribute to the challenge. The different priorities and ways of thinking of nuclear plant personnel, who are operational technology (OT) engineers, and cyber security personnel, who are information technology (IT) engineers, frequently lead to misunderstandings. The problem is exacerbated by the fact that cyber security personnel are often located at a considerable distance from nuclear facilities and rarely visit.

Furthermore, the level and quality of cyber security training at nuclear facilities are insufficient: in addition to a lack of cyber drills, nuclear personnel may have a poor understanding of key procedures, in part as a consequence of the cultural divide, since the training material is written by IT engineers. Thus nuclear plants may lack preparedness for a large-scale cyber security emergency, particularly one that occurs after normal working hours.

There are numerous technical challenges too. Having been designed in the 1960s when the idea that a malicious actor would try to attack them was inconceivable, many industrial control systems lack basic security measures such as authentication and encryption, making them 'insecure by design'. Moreover, the flexibility of code means that any attacker who can get past network perimeter defences can make logic changes that are very difficult to spot. And standard cyber security solutions used in home or office IT environments, such as patching, are much more difficult to implement in nuclear facilities. Supply chain contamination is also a concern.

Growing recognition of the rapidly changing cyber security scene led the International Security Department at Chatham House to undertake an 18-month project exploring the potential impact on and implications for the civil nuclear sector. The project sought to assess the major cyber security challenges and risks posed to nuclear facilities and nuclear power plants in particular; identify international policy measures that could help to enhance cyber security at nuclear facilities; and increase knowledge and awareness among both industry practitioners and policy-makers of cyber security concerns in the nuclear sector. This report focuses on the major cyber threats to nuclear facilities, in particular on those that could affect industrial control systems, and suggests potential responses and solutions.

Methodology

The research took a fourfold approach: a literature review; interviews with industry practitioners, policy-makers and academics; a series of expert roundtable workshops at Chatham House; and soliciting feedback from industry experts at international conferences.

Literature review. Since the current literature on the cyber security threats to nuclear facilities is relatively limited, the project drew on a wide range of sources, including academic publications, industry reports and news articles. The related literature on the cyber security risks to critical infrastructure was also consulted (see Select Bibliography).

Interviews. Interviews were conducted with 30 practitioners (each referred to in the text as a numbered source) working on cyber security and on nuclear issues in fields ranging from industry to government, international organizations and academia. Since the project's remit was international, interviews were conducted with experts from several different countries, including the United States, United Kingdom, Canada, France, Germany, Japan, Ukraine and Russia, as well as representatives of major international organizations, including the IAEA and the European Network and Information Security Agency (ENISA). They included both industrial control systems experts and IT experts working in the nuclear field; a former manager at two US nuclear plants; a former security manager at the UK Civil Nuclear Constabulary; a cyber security practitioner at the owner-operator of several Canadian nuclear plants; a cyber security practitioner at the owner-operator of a large number of French nuclear plants; and a Japanese vendor of equipment for nuclear facilities. The sources have been cited anonymously. Several of them did not wish to be quoted at all, some were willing to be quoted but without being named, and others were happy to be identified. In order to ensure anonymity for those who require or desire it, the report does not identify any source by name.

Expert roundtable workshops. Three roundtable meetings were held at Chatham House – in May 2014, September 2014 and April 2015 – to bring together cyber and nuclear experts from both industry and government. Summary reports fed into the analysis in this report.[1]

Presentation of research and feedback. Chatham House has already presented early project findings and solicited feedback from experts at two NATO Advanced Research Workshops. The first, on 'Strengthening Cyber Security for Critical Infrastructure', was held on 30–31 October 2014 in Kiev, and the second, on 'The Protection of Critical Energy Infrastructures Against Emerging Security Challenges', took place on 26–28 November 2014 in Tbilisi. The project team also took part in the IAEA's first major international meeting on cyber security issues, the 'IAEA International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange', on 1–5 June 2015 in Vienna.

[1] In order to communicate with and involve the wider community, the project also has both a webpage at http://www.chathamhouse.org/about/structure/international-security-department/cyber-and-nuclear-security-project and a blog at http://cyber-and-nuclear-security.blogspot.co.uk/.

2. Background: the Nature of the Threats

Summary

This chapter examines known cyber security incidents at nuclear facilities and their consequences, and describes the various threat actors ranging from hacktivists to states. It also details the possible impacts of a cyber attack, which cover the spectrum from the theft of commercial data to the release of ionizing radiation.

Recent incidents

Recent high-profile cyber attacks on nuclear facilities have raised new concerns about the vulnerability of nuclear power plants. In 2010, the emergence of the Stuxnet worm heralded the advent of a new era in cyber warfare. In a cyber attack on the Natanz nuclear enrichment facility and Bushehr nuclear power plant in Iran, the Stuxnet worm caused the partial destruction of around 1,000 centrifuges (Shubert, 2011). This was the most highly sophisticated publicly known cyber attack on a nuclear facility to date, demonstrating an unprecedented level of technical capabilities. On a lesser scale, South Korea's state-run nuclear operator was the subject of a cyber attack in December 2014 which saw the theft of sensitive information, including the blueprints of at least two nuclear reactors and electrical flow charts (Kim and Cho, 2014).

Non-cyber security-related serious incidents, such as the damage inflicted on the Fukushima Daiichi nuclear power plant by the magnitude 9.0 Tōhoku earthquake and subsequent tsunami on 11 March 2011 (von Hippel, 2011), serve as a stark reminder of the economic and social consequences of a major disruption to or disablement of a nuclear power plant's essential systems, in this case the reactor cooling systems. Over 100,000 people within a radius of 20 km were evacuated and those within a radius of 20–30 km were instructed to shelter before later being advised to evacuate on a voluntary basis. Restrictions were placed on the distribution and consumption of food and the consumption of drinking water (IAEA, 2015). Large areas of prime agricultural land continue to be uninhabitable; and the nuclear operator and the Japanese government still have to cope with the task of controlling the radiation release and clearing the radioactive contamination. The wider consequences of the accident included the shutdown of all nuclear power plants in Japan at the time, leading to significant energy supply problems for the population. The ramifications were felt elsewhere too: for example, the German federal government ordered the shutdown of eight of the 17 German nuclear reactors and immediately pledged to close the rest by 2022 (Breidthardt, 2011).

Box 1: Known cyber security incidents at nuclear facilities

Ignalina nuclear power plant (1992)
As early as 1992, a technician at the Ignalina nuclear power plant in Lithuania intentionally introduced a virus into the industrial control system. He claimed this was in order to highlight the cyber security vulnerabilities of such plants, although this did not stop the police from arresting him. It also illustrates the dangers of the insider threat – in this case little harm was caused, but someone with malicious intent could have provoked a serious incident. Speaking about it at a conference three years later, Russian Security Council Deputy Secretary Valentin Sobolev warned: 'An interconnection between nuclear terrorism and cyber terrorism could have a global catastrophic nature … The hacking of a computer at the Ignalina nuclear power plant in Lithuania could have resulted in a disaster similar to that in Chernobyl' (NTI, 2006; Bukharin 1997).

Davis-Besse nuclear power plant (2003)
In January 2003, the Davis-Besse nuclear power plant in Ohio was infected by the Slammer worm (also called W32/SQLSlam-A or Sapphire). Slammer spread rapidly to computers across the internet by exploiting a vulnerability in the Microsoft SQL 2000 database server software. The worm scans and sends itself to random IP addresses; if it reaches a machine that is running Microsoft SQL 2000, it infects that machine and begins scanning and sending itself anew.

Slammer found its way to Davis-Besse by first infecting a consultant's network. From there it infected the corporate network of First Energy Nuclear, which operates the plant. First Energy Nuclear's corporate network was connected directly to a supervisory control and data acquisition (SCADA) system at Davis-Besse so that it could remotely monitor the plant, without any type of firewall. Once on the corporate network, Slammer could thus make the jump onto the SCADA system. It then generated a large amount of traffic that overwhelmed the system. The safety parameter display system (SPDS), which collects and displays data about the reactor core from the coolant systems, temperature sensors and radiation detectors, was unavailable for almost five hours.

Fortunately, Davis-Besse's reactor was not in operation at the time, but the same scenario could have occurred if it had been. A patch for the Microsoft SQL 2000 vulnerability, which had been released six months earlier, would have prevented infection by Slammer, but neither the corporate network nor the SCADA system had been patched (Kesler, 2011).

Browns Ferry nuclear power plant (2006)
In August 2006, the Browns Ferry nuclear plant in Alabama experienced a malfunction of both the reactor recirculation pumps (which use variable-frequency drives to control motor speed and are needed to cool the reactor) and the condensate demineralizer controller (a type of programmable logic controller or PLC). Both of these devices contain microprocessors that send and receive data over an ethernet network, but this makes them susceptible to failure if they receive too much traffic. (Ethernet functions by sending data to every device on the network; the network devices then have to examine each packet to determine if the packet is destined for them or if they can ignore it.) At Browns Ferry, it seems that the network produced excess traffic that caused the reactor recirculation pumps and condensate demineralizer controller to fail. The plant's Unit 3 then had to be manually shut down in order to avoid a meltdown (Kesler, 2011).

Although this was not a cyber attack, the incident reveals the impact that the failure of just one or two devices can have on a plant. It also suggests that if a hacker were to cause a recirculation pump to fail, it could seriously disrupt plant operations. Such an attack mounted in combination with infection by a worm like Slammer could disable not just the recirculation pumps but also the sensors that warn plant personnel of a problem – which would pose a serious threat (Kesler, 2011).

Hatch nuclear power plant (2008)
In March 2008, the Hatch nuclear power plant in Georgia experienced a shutdown as an unintended consequence of a contractor update. An engineer from Southern Company, the contractor that manages the plant's technology operations, installed an update to a computer on the plant's business network. The computer was connected to one of the plant's industrial control system networks, and the update was designed to synchronize data between the two. As a result, when the engineer restarted the computer he had updated, the synchronization reset the control system's data to zero for a brief moment. However, the plant's safety system incorrectly interpreted the temporary zero value of the water level to mean that there was insufficient water to cool the reactor core, putting the plant's Unit 2 into automatic shutdown for 48 hours (Krebs, 2008).

This demonstrates that nuclear owner-operators often do not understand the full ramifications of connecting their business networks to a plant's industrial control systems. Although in this instance the update's unforeseen consequences did not put the plant in danger (although it did trigger a costly shutdown), it shows how a hacker might make a change to a plant's business network that, either unintentionally or intentionally, could have a significant impact on industrial control systems (Kesler, 2011).

Natanz nuclear facility and Bushehr nuclear power plant – Stuxnet (2010)
First exposed publicly in June 2010, the Stuxnet computer worm infected both the Natanz nuclear facility and the Bushehr nuclear power plant in Iran, partially destroying around 1,000 centrifuges at Natanz. It is believed to have been designed by the US and Israeli governments and specifically targeted to disrupt Iran's uranium enrichment programme (Anderson, 2012).

The worm most likely spread initially when infected USB flash drives were introduced into these facilities, which thus became infected despite being 'air gapped' (i.e. fully separate from the public internet).

Stuxnet infects computers that run the Microsoft Windows operating system, taking advantage of vulnerabilities in the system that allow it to obtain system-level access. (The worm also makes use of falsified certificates so that the files it installs appear to come from a legitimate company, thus deceiving antivirus software.)

Once it has infected a machine, Stuxnet checks to see if that computer is attached to a Siemens Step 7 SCADA system, as used by Iranian nuclear facilities. If the computer is not attached to such a system, then no payload is activated. Instead, Stuxnet continues to replicate itself on other computers. One way it does this is by taking advantage of another set of vulnerabilities in print spoolers to spread to networks with shared printers. And of course it continues to spread through USB flash drives.

If the computer is attached to such a Siemens system, then Stuxnet's payload is activated and it reprogrammes the system's PLCs, which control centrifuges used to enrich nuclear fuel, so that they spin too fast and eventually break apart. At the same time, it also sends false feedback to make it appear as if the system is running properly (Falliere et al., 2011).

Stuxnet was aimed at preventing the acquisition of a nuclear weapons programme, not causing an explosion or inflicting civilian casualties, but its unprecedented capabilities show the destructive potential of such technologies if used for more nefarious purposes, and have heralded a new era in cyber attacks as other countries race to develop offensive cyber capabilities.

Unnamed Russian nuclear power plant – Stuxnet (circa 2010)
Stuxnet is also believed to have infected a Russian nuclear power plant during 'the Stuxnet time', around 2010. This incident was revealed by Eugene Kaspersky, founder and CEO of Kaspersky Lab, during a question-and-answer session after a 2013 talk. He reported that a friend who was working at the nuclear plant at the time told him that the plant's internal network – which was air gapped – was 'badly infected by Stuxnet'. The plant has not been identified.

As Kaspersky pointed out, this incident shows the unintended consequences that state-sponsored malware can have. Even though Stuxnet was narrowly targeted, it still infected at least one other plant. He added: 'Unfortunately, it's very possible that other nations which are not in a conflict will be victims of cyber attacks on critical infrastructure' (Kaspersky, 2013). This incident also confirms that an air gap is no guarantee of protection.

Korea Hydro and Nuclear Power Co. commercial network (2014)

In December 2014, hackers infiltrated and stole data from the commercial network of Korea Hydro and Nuclear Power Co., which operates 23 of South Korea's nuclear reactors (Cho, 2014). The hackers gained access by sending phishing emails to the owner-operator's employees, some of whom clicked on the links and downloaded the malware. The hackers obtained the blueprints and manuals of two reactors, most likely belonging to the Gori and Wolseong nuclear power plants, as well as electricity flow charts, personal data belonging to some 10,000 of the company's employees, and radiation exposure estimates for inhabitants in the surrounding area. The data were leaked over Twitter from an account purported to belong to the head of an anti-nuclear group in Hawaii; the hackers also warned Korea Hydro and Nuclear Power Co. to shut down three reactors or face 'destruction'. The owner-operator ignored the ultimatum, which turned out to be an empty threat (Kim and Cho, 2014).

Further blueprints and test data were leaked over Twitter in March 2015, with the hackers demanding money in order not to release more data and intimating that other countries had expressed interest in purchasing the data. Rather than responding, South Korea issued a statement officially blaming North Korea for the attack, citing as evidence that IP addresses used in the phishing attacks were linked to the regime; North Korea has strenuously denied the accusations (Park and Cho, 2015).

The incident illustrates the rise in extortion in the nuclear industry. Those interviewed for the project have reported that such incidents, while not often publicly known, are relatively frequent.

The range of threat actors

The primary set of threat actors that pose a cyber risk to nuclear facilities can be divided into four broad categories: hacktivists; cyber criminals; states (governments and militaries); and non-state armed groups (terrorists).

Hacktivists such as radical fringe anti-nuclear power groups might carry out a cyber attack on a nuclear facility to raise awareness of vulnerabilities. Their goal is sabotage or disruption, so such attacks would be likely to involve defacements of websites or low-level attacks on the business network intended to embarrass an operator rather than cause a dangerous incident.

Cyber criminal groups are becoming increasingly skilled. Organized criminal groups might steal confidential information belonging to a nuclear facility and then blackmail the facility into paying a ransom to prevent it from being released. Their primary aim is monetary profit (Source 26).

The threat from state actors ranging from intelligence agencies to militaries and state-sponsored groups is on the rise (McConnell et al., 2014). These types of attackers tend to instigate long-term campaigns aimed at infiltrating the critical infrastructure of other countries (Source 25). Currently the activities of states occur more in the area of cyber espionage than cyber conflict. According to Source 1: 'At present, the motivations are primarily commercial, aimed at the theft of sensitive, confidential proprietary data that will give the country an advantage.' Yet in the longer term, the unintended escalation of cyber skirmishes into cyber conflict is a concern. These same infiltration campaigns are also aimed at acquiring cyber capabilities against the critical infrastructure of other states, including nuclear plants, in the event of a conflict (Source 25). In such a case, the intent of an attack might be to endanger human or environmental safety or, at the very least, to create widespread confusion and fear among an adversary's population.

Terrorists or non-state armed groups are a growing challenge. Some radical extremist groups have already acquired significant capability in the use of social media and, with sufficient financial resources, could develop the capability to carry out a cyber attack on a nuclear plant or employ a 'hack for hire' company to do this (BBC, 2011). For example, ISIS (Islamic State of Iraq and Syria), with its sophisticated use of Facebook and websites for recruiting purposes, could potentially pose such a threat. According to Source 10:

> Radical extremism is also a serious risk, so we can consider it at least equal [to a] governmental hack attack. If an attacker really wants to penetrate or infiltrate the network, it is a question of time and money.

Such groups might wish to build up a picture to support a later coordinated attack intended to sabotage the plant or to remove nuclear material. Or they might wish to use cyber means in order to cause physical destruction.

Potential physical targets and impacts

There are a number of ways in which cyber attacks might affect nuclear facilities. Some of the most important targets are detailed below.

The most basic attacks will target business networks – the corporate networks belonging to the owner-operators of nuclear facilities that contain the information needed to manage the business dimension of the plant. Most attacks on these networks will be aimed at the theft of confidential corporate data that can be used to garner financial benefit. Others might be carried out for reconnaissance purposes, to steal operational information that can be used to conduct a more harmful attack at a later date. Or, as business networks are typically connected to the nuclear facility, some attacks on business networks could serve as a route for attacks on the facility's industrial control systems.

A cyber attack that took one or more nuclear facilities offline could, in a very short time, remove a significant base component to the grid, causing instability.

More sophisticated attacks on nuclear plants involve the targeting of industrial control systems themselves and have the potential to be the most harmful. Within the plant itself, the industrial control systems are the most important, notably SCADA systems. While highly complex, these can be thought of as having just three parts. The first consists of the computers that control and monitor plant operations, and that send signals which physically control the second part. This comprises the field devices, such as programmable logic controllers, which control the sensors, motors and other physical components of the plant. The third part consists of the human–machine interface (HMI) computers which display user-friendly data on operations and often run using Windows programmes.

Some possible attack scenarios might include the following.

A cyber attack on a nuclear plant could cause a widespread loss of power. Nuclear reactors using water in their primary cooling circuit are designed to give a high level of protection to that water, but the water supply that cools the turbines which in turn generate the electricity is not so well protected. Without that water supply, the turbine could be tripped and electricity generation halted, with a serious impact on the power grid. In countries that rely on nuclear energy, power provided by nuclear plants is considered to be the 'base load', or a steady and constant source of supply. Other sources of power generation, for example gas-fired electricity generation, can be more responsive to demand and so can be adjusted to meet peaks in demand and to reduce supply when there is a lower requirement for power. Thus a cyber attack that took one or more nuclear facilities offline could, in a very short time, remove a significant base component to the grid, causing instability. According to Source 27:

> In the US, it's very easy to have this ripple effect because if those plants go off the grid quickly enough, it's a pretty significant percentage of the grid's base load that all of a sudden disappears, which causes the entire grid to become burdened. If you did that to a reasonable number of those larger substations, you could cause a significant grid event.

The consequences of a loss of power could be severe.

In theory, **a cyber attack on a nuclear plant could bring about an uncontrolled release of ionizing radiation.** An adversary with sufficient technical knowledge and adequate resources could mount an attack on a nuclear power plant that could trigger the release of significant quantities of ionizing radiation. All nuclear power plants need offsite power to operate safely and all have a standby generator system which is designed to be activated when a loss of mains power occurs. Attacks on the offsite power supply and the on-site backup system could create some of the effects that occurred following the 2011 earthquake and tsunami at Fukushima Daiichi, although multiple failures of the many safety features at modern nuclear power plants would also need to occur at the same time as that loss of offsite power and the disruption of standby generators.

The risk of **simultaneous attacks** is also a concern. It is possible that different types of attacks could be launched simultaneously against a nuclear plant: for example, a cyber attack might be planned to occur concurrently with a physical, perhaps armed, intrusion on the same plant. Alternatively, there could be a concerted simultaneous cyber attack on a nuclear facility and on other types of critical infrastructure such as regional water systems, the electrical grid or banking systems.

Box 2: Cyber conflict

The changing nature of the cyber security threat appears to have prompted some countries to begin overtly and rapidly preparing defensive and offensive capabilities in the event of a future conflict that includes cyber attacks between states (McConnell et al., 2014). If such a conflict were to occur, nuclear power generation plants could well be prime targets.

Potential attackers are likely to be states, but it is possible that non-state armed groups with sufficient financial and other resources may turn to cyber attacks. Cyber defence requires significant financial and intellectual investment, and states that lack such resources or are reluctant to commit them may become increasingly vulnerable to attack.

Attackers would face two challenges. First, their cyber attack would have to be tailor-made for the specific target plant, which would require knowing exactly which software programmes run the control systems. Obtaining this information is difficult and time-consuming. It would involve reconnaissance of the plant in advance, stealing passwords or obtaining insider intelligence.

Second, they would need a customized test-bed – which would be very expensive – to trial such a weapon. At present only the most advanced states have this capability.

A state-sponsored cyber attack on a nuclear facility of another state would attract widespread international condemnation and invite reprisal. This would deter most states – although not all. The difficulty of attribution means that the perpetrator might not be identified.

> It is not like you are having tanks coming over the hill, or you've got soldiers in uniforms flying flags; the reality is we're seeing a real increase in the use of false flag operations. Attacks that appear to be coming from somewhere are actually coming from somewhere else. (Source 26)

In the midst of a wider, physical interstate conflict, however, cyber attacks against a range of critical infrastructure including nuclear power plants would have to be considered possible, and even probable. Numerous countries are rapidly acquiring cyber capabilities to attack critical infrastructure, and nuclear plants could become targets of choice in an all-out attack.

3. A Growing Threat – and an Evolving Industry

Summary

This chapter describes the growth of the cyber security challenge in the nuclear industry. There are ever more tools and services that make it easier and cheaper for hackers to attack industrial control systems, including at nuclear facilities: search engines can readily identify critical infrastructure that is connected to the internet, techniques from Stuxnet are being copied, and automatic cyber attack packages targeted at known and discovered vulnerabilities are widely available for purchase. In parallel, there is a rise in factors that make nuclear facilities more vulnerable to cyber attack, with facilities increasingly adopting digital systems, making use of commercial off-the-shelf software, and connecting to the internet. All of these offer considerable cost savings but are easier to hack.

Because of this rapid evolution, nuclear facility personnel do not necessarily understand the extent of facilities' vulnerability to cyber security threats. Many still cling to the myth that nuclear facilities are 'air gapped' – and that this protects them from cyber attack. Furthermore, nuclear personnel may not always realize that nuclear facilities may have internet connectivity: VPN connections are increasingly used, and there are sometimes undocumented or forgotten connections installed by contractors and other legitimate third-party operators without malicious intention.

Growth in the abilities of cybercriminals

A number of factors have made it easier and cheaper than ever for hackers to attack critical infrastructure, including nuclear facilities. The **growth in specialized search engines for internet-connected industrial systems** is one such element. For example, the search engine Shodan, which allows users to search for and find SCADA systems that are connected to the internet, has grown in popularity. According to Source 25:

> We did research in which we used Shodan and found all of the nuclear plants in France that are connected to the internet. If a user knows what he is looking for, he could easily find this information.

Specifically, Shodan's geolocation capability can display the location of the identified SCADA systems on a map. Taking this with known facts such as the location of nuclear plants in France, it is entirely possible to correlate the two datasets and to determine which of those identified SCADA systems are at nuclear facilities. The basic version of the search engine is free to use, while more extended searches are not onerous. Another search engine, ERIPP, is very similar to Shodan but concentrates on critical infrastructure.

Once the user has identified the internet-connected systems at a nuclear facility, it may be possible to take advantage of default passwords to gain access. Some nuclear facilities do not change the default passwords on their equipment, yet those used by companies such as Honeywell and Siemens are widely shared on hacker websites. 'You know that for company X, the default password is always, say, 1234, so you can get in that way,' comments Source 25. Thus hackers can often gain access more easily than managers of nuclear facilities expect.

Another element is that **cybercriminals are now able to copy the advanced techniques used by Stuxnet**. Stuxnet's tactics, which could only have been developed by a team from a highly advanced state, are now known to less skilled hackers who would not have had the capability to develop such sophisticated malware on their own. Once Stuxnet's existence became publicly known, hackers around the world took inspiration from the way it functioned and incorporated some of its features into malware to suit their own purposes. The same techniques could be adopted to launch attacks on other nuclear facilities (Simonite, 2012).

Moreover, the **increased availability of automated exploit toolkits** is making it easier for hackers to attack industrial control systems (Zetter, 2014). For example, open source toolkits such as the Metasploit Framework – which is free to use – enable users to use and execute any exploit combined with any payload in order to test a system for vulnerabilities.[2] The framework was originally designed to automate the process of penetration testing, but hackers can now use these same exploits to attack a system by simply replacing the payload with a malicious one. In the past, they had to develop their own tools, so only a small number of highly skilled hackers were able to attack industrial control systems. Now automated exploit toolkits not only make it easier for less skilled hackers to engage in such attacks, but also automate the process.

Furthermore, **an increasing number of companies are selling zero-day vulnerabilities**[3] and exploits that take advantage of these. Rather than reporting the vulnerabilities to the software vendors so that they can be patched, they are selling them to governments and to other paying customers instead. As an example, ReVuln, a company based in Malta, specializes in selling zero-day vulnerabilities for SCADA systems. This type of activity is currently not illegal because such companies are operating in unregulated 'grey markets'.

[2] An exploit is a software tool that takes advantage of a vulnerability in a computer system; the payload is the malicious code that it installs.
[3] Zero-day vulnerabilities are gaps in computer security that are unknown to anyone except the researcher who found them; that is, they have been known about for zero days.

Growth in vulnerabilities in nuclear facilities

At the same time, several factors are increasing the vulnerability of nuclear facilities to cyber attack. One is the **increasing use of digital systems,** which are more susceptible to cyber attack. Many nuclear plants were built in the 1960s, 1970s and 1980s, and are primarily legacy analogue systems comprised of hardware and software designed during those decades. Although much of this older equipment lacks important cyber security features, the systems have, for many years, provided a certain form of 'protection by antiquity'. In the years before the arrival of microprocessors, systems were hardwired, which means that a computer's logical functions were carried out by circuits that were permanently built into devices, instead of by programmable code. They had so little flexibility that any attacker wanting to change a device's function would have had to go to the device and make a physical change to the circuit. And many of these older systems predate networking, so network-based attacks are not possible.

As older equipment in existing facilities reaches the end of its working life and needs replacement, comparable equipment is no longer manufactured or available, and so it is gradually being replaced with newer hardware (and software) that has more digital features. Now, the use of programmable code means that an attacker can simply change the code in order to change the function of a device; digital systems allow an unprecedented amount of flexibility, which makes them more susceptible to cyber attack.

> With the advent of the microprocessor, there are so many degrees of freedom you can do anything you like. Before that, systems were hardwired. What they did was built into the design and so there was not much flexibility. That means that there was very little scope for subverting them or for them doing the wrong thing. (Source 5)

Furthermore, these new digital systems have been conceived without adequate security protection, making them 'insecure by design' (this concept is discussed further in Chapter 6). Thus new industrial control systems and new-build nuclear power plants dependent on these digitized technologies are more susceptible to cyber attacks that exploit these weaknesses.

> There is more and more automation coming into the nuclear industry because of obsolescence. So there are more and more cyber-sensitive systems being installed. The problem is these systems often haven't been adequately designed. (Source 8)

> Whatever technology is currently available will provide the raw materials for what gets put around these reactors, and there are some fundamental problems with the way that the digital system that we have got is engineered. It is not actually a sound basis on which to build safety-critical systems. (Source 5)

In addition, there appears to be some **reduction in the level of redundancy** (the addition of extra critical components or functions to provide backup should a component fail) currently existing in nuclear facilities. A key redundancy requirement is for fail-safes, which ensure that if a system should fail, it does so in a safe manner. As nuclear facilities gradually convert from analogue to digital, fail-safes are losing part of their efficacy: since the digital systems are not independent, there is no longer a genuine redundancy.

> Fail-safes used to be hardwired, analogue, completely set aside from anything else; you wanted to make absolutely sure they would work. But with the microprocessor, it is now cheaper to incorporate both control and safety in the same device. We are losing redundancy. (Source 8)

Another factor is **the increasing use of commercial off-the-shelf systems** that are easier to hack. The nuclear plants built between the 1960s and 1980s run highly customized SCADA systems. The large number of vendors meant that systems, computer languages and proprietary protocols varied widely from plant to plant. This provided 'protection by obscurity'. Attacking such individualized systems is difficult: hackers would first need to acquire specific knowledge of a SCADA system's particular characteristics, which might require insider information; then they would have to identify vulnerabilities in order to write and deliver exploits to take advantage of these. And they would have to do this for each plant they wanted to attack.

Since the 1990s, facilities have been increasingly integrating their SCADA systems with computer networks built from commercial operating systems such as Windows or Linux, manufactured by a small number of vendors (Kesler, 2011). This offers cost savings and greater efficiency, but the growing use of these operating systems in a large number of industries across the world means that hackers are already familiar with their vulnerabilities and previously written exploits that they can use. Hackers are thus able to attack nuclear plants with far less effort and a much greater chance of success.

Furthermore, **the use of 'air gaps' is declining at nuclear facilities,** which opens up new vulnerabilities for cyber attack. Traditionally, being air gapped, or fully isolated from the public internet, has formed the mainstay of nuclear facilities' defence against cyber attacks. This literal gap of air between the nuclear plant and the public internet provided a form of 'protection by isolation'.

Yet in recent years many nuclear facilities have gradually developed some form of internet connectivity. This is in large part because legitimate third parties located off-site (and often some considerable distance away) need access to data generated at the plant. Owner-operators are increasingly opting to use the internet to transfer such data because it is the most efficient way of doing so; they find it too slow and cumbersome to download the data onto a USB drive which is then sent to those who need it.

The third parties requiring access include the owner-operators' head offices which, for reasons of efficiency, need to receive and analyse large amounts of data on how a plant is functioning. There are regulatory needs as well: government regulatory agencies, and possibly Computer Emergency Response Teams (CERTs), require rapid access to diagnostics in case of a plant malfunction. These third parties increasingly include vendors as well.

> Twenty-five or thirty years ago we did everything via phone. But now, head organizations want to get data in real time. So the only thing is just to connect to the internet. (Source 10)

In most cases, third parties only need to download data from the plant. However, there may also be instances in which they wish to upload data – for example, vendors may wish to undertake software updates remotely. Since each facility has several suppliers, this means that a large number of actors may need to connect to nuclear facilities.

> While you see the notion of the air gap in the literature … it used to be true but in practice it is less and less the case. Today there are many third-party vendors that want remote access to do updates and monitoring. (Source 25)

> Most equipment manufacturers can remotely monitor a device for problems. And all of the plants have several suppliers, so that's a lot of people who are connecting. (Source 10)

Modes of cyber infection

Infection via known connections to the internet

Nuclear facilities that allow third-party remote access may open up several new avenues by which hackers can gain access. **The owner-operator's commercial network can serve as a route of infection.** Owner-operators are increasingly creating direct links between their corporate business networks and facilities' industrial control system networks. In many cases, the plants will employ optical data diodes, which allow unidirectional communication (i.e. allow data to flow outwards but not inwards) by beaming a laser through a fibre optic cable from inside the plant to an external receiver. The receiver detects the light and converts it into data form; it has no ability to transmit data back, making the system nearly impossible to breach (except perhaps by a highly advanced state actor).

In other instances, however, these links may not be adequately protected and a hacker may be able to use the corporate business network to gain access to the nuclear facility's industrial control systems. For example, some nuclear facilities may only be using a firewall (which controls incoming or outgoing traffic according to a set of rules), configured so that it only allows traffic to flow outwards, to protect the industrial control system network. Yet it would be relatively straightforward for a hacker to modify the firewall settings and gain access.

> As standards vary from country to country, so will the technologies. The companies that are aware of the need to do the right thing implement data diodes. But not everybody implements data diodes, which means that there is room for interpretation with the regulations as you go from country to country. (Source 27)

Virtual private networks can also provide one possible route of infection; some plants are permitting vendors to access facilities remotely through a VPN connection, which allows individuals to connect to a private network over the internet via a secure encrypted tunnel. If the VPN is insecure, however, it can be a source of vulnerability, making it possible for malware to find its way onto the industrial control network.[4]

For example, if VPN access is allowed to the digital reactor protection system, which is the system that shuts down the reactor in the event of a safety concern, a hacker could gain access to and compromise the reactor protection system, triggering a plant shutdown – or, worse, preventing a plant from shutting down in response to a safety alert.

> There are some countries that allow remote access for the vendors to the digital reactor protection systems. And if a hacker knows that, he has an entry point. (Source 30)

VPNs can also be an avenue for unintentional infection of a facility. As noted in Box 1 above, at the Davis-Besse nuclear plant in 2003, an engineer working for a subcontractor connected from his home laptop via a VPN to his company, and that company had a site-to-site VPN with the nuclear plant. His home laptop was infected with malware, infecting the facility and causing a monitoring system to crash. Fortunately, Davis-Besse was shut down at the time, but as this is a standard way of providing remote access, the same scenario could be repeated elsewhere (Kesler, 2011).

Infection via undocumented connections to the internet

Often, nuclear facilities will have undocumented connections to the internet (i.e. connections of which the plant managers or owner-operators are unaware); these too can provide potential pathways through which malware can infect a nuclear facility.[5]

[4] Instead of using VPNs, nuclear facilities could build a private cable connection to third parties, but this would be prohibitively expensive, particularly given the number of third parties that would want access. And even a private cable connection could be tapped, although this would possibly require state-actor capabilities and physical access to the cable.

[5] For this reason, network diagrams of nuclear facilities that map out existing connections are frequently incorrect; there are often a number of additional connections that have not been documented.

In some cases, **contractors or employees might set up rogue or unauthorized connections** (Source 10). For example, even though wireless connections are generally strictly forbidden at nuclear facilities, a contractor might – for reasons of convenience – install a wireless network in the office without informing systems administrators. If that wireless network is not adequately protected, a hacker could access (or malware might infect) an industrial control system through the office network wireless.

A related concern is that contractors or employees might install temporary internet connections and then forget about them. For example, a contractor providing maintenance might add a router and use it only once for a specific purpose; then if it not removed once the task is finished, its installation could easily be forgotten and that internet connection could provide an avenue for infection (Source 28).

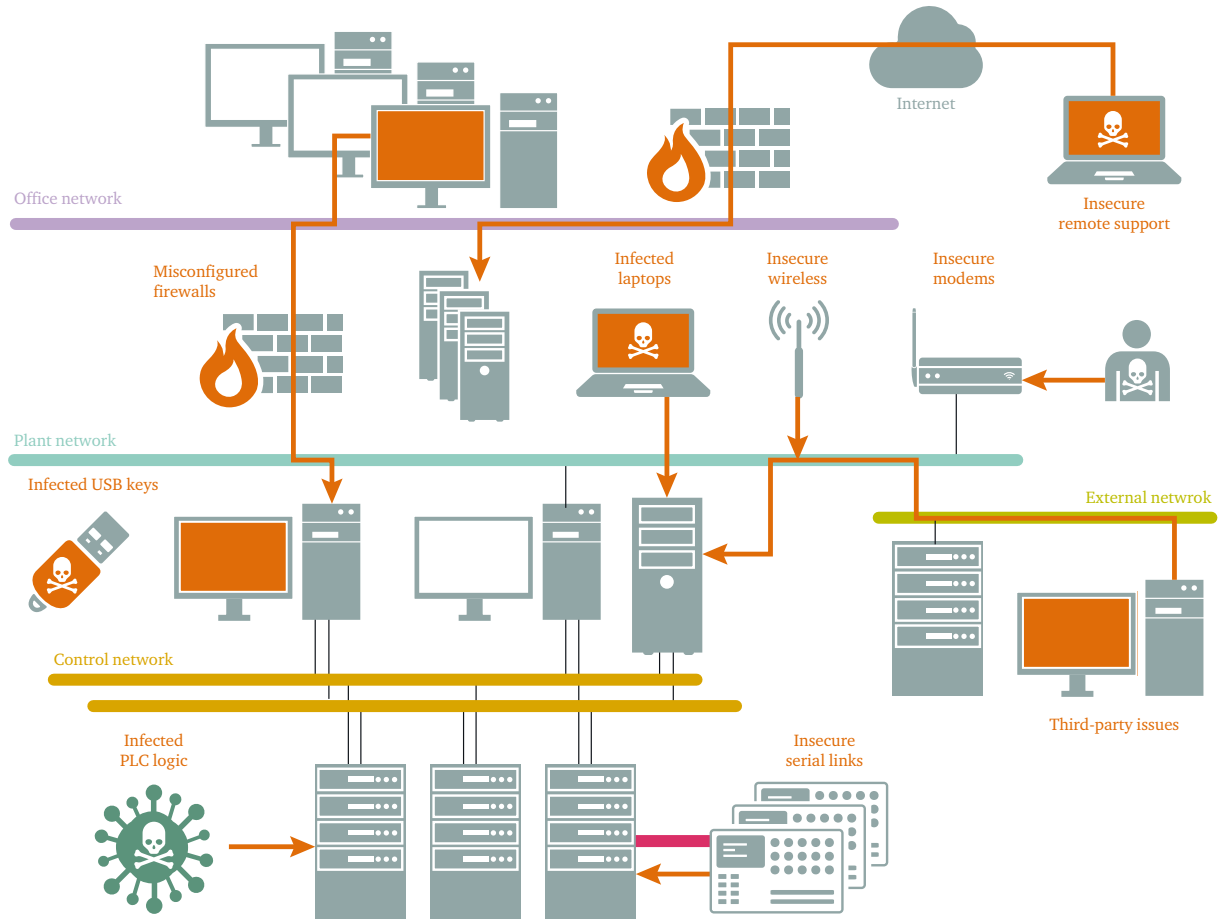
> The maintenance team can be part of the problem. How do we prevent somebody from putting in a wireless access point and plugging it in? It's basically to make their lives easier. (Source 26)

In some instances, **contractors or employees might inadvertently install equipment that has internet connectivity.** For example, when a part wears out in a facility, a contractor might replace it with a new part that could have exactly the same serial number as the old part, leading the contractor to believe that it is exactly the same. Yet the vendor might have added a Wi-Fi or GPS functionality that provides a mode of access for a hacker (or malware).

Infection despite being air gapped

Even when nuclear facilities are air gapped, there are still a number of possible routes of infection; while an air gap does reduce a facility's vulnerability, it does not provide complete protection. For example, **malware can infect a nuclear facility when a USB drive or other removable media device is plugged into the plant network.** If the removable media device contains malware, it can spread to the plant itself. This was the most likely route by which the Stuxnet worm infected the Iranian nuclear facilities at Natanz and Bushehr, which were both air gapped.

Figure 1: Potential control system vulnerabilities



Source: Eric Byres, Byres Security.

As discussed previously, given that nuclear facilities will always have a need to either download data (e.g. to get data off the plant) or, perhaps less frequently, to upload data (e.g. to perform a software upgrade), this will require the use of removable media devices in the case of air gapped facilities – thus breaching the air gap.

> Information still needs to flow inbound periodically, whether you use a USB or something else, and that's where problems can occur. (Source 9)

The DragonFly cyber espionage campaign – also known as Havex or Energetic Bear – which targeted US and European energy companies (although there are no reports of nuclear facilities specifically having been infected) provides an example of how malware can be introduced via software updates. The attack infected the software updates of SCADA equipment manufacturers with a Trojan Horse malware program. When energy companies installed these software updates, the malware spread to facilities' industrial control systems, giving the hackers backdoor access.

In other instances, nuclear plant personnel might, for reasons of convenience, bring their own USB drives or other removable devices into a plant and use them to transfer data, thereby providing an opportunity for malware to cross the air gap.

> Air gaps work in theory, but not in practice. All it takes is a USB drive: people walk into the plant room, plug the USB into the system, and the malware is on there. All of a sudden it has jumped the air gap. (Source 26)

> If you allow in a USB key, which breaches the air gap, you've now got a connection that nobody really considered. And since there is [often] no security software running on any system machines, malware is free to do whatever it wants. (Source 27)

Figure 1 shows typical points of vulnerability in industrial control systems.

Misunderstanding connectivity

Despite the demise of the air gap within many nuclear facilities today, **a number of nuclear plant personnel and even owner-operators of facilities may not necessarily realize that their nuclear facilities have internet connectivity – or fully understand its implications.**

> We have this tired cliché that industrial control systems aren't connected to the internet. But search engines like Shodan have proved that they are. (Source 26)

> Many nuclear operators say that their facilities are not connected to the internet, so there is no risk. (Source 25)

Differences in terminology may contribute to this confusion. While the 'true' definition of an air gap is a literal gap of air between a nuclear facility and the public internet, the term is increasingly used to describe facilities that have a unidirectional connection, yet depending on the type of technology used, such a connection could be vulnerable to hacking.

Moreover, many plant personnel and owner-operators fail to realize that, even if they are air gapped, this does not protect them from cyber attack.

Source 26 points out:

> The common rhetoric I hear within the nuclear industry is, 'We don't need to worry about a cyber attack because our plant is air gapped.'

There appears to be some element of denial. Some nuclear facility personnel may view cyber conflict as occurring between a small number of advanced states rather than as a threat that concerns them. Source 25 explains:

> For them, it remains a movie scenario, maybe in the future. They think it is just states against states, not everybody wants to hack us, and also it won't happen here.

Furthermore, many in the industry are also sceptical about the potential for a release of ionizing radiation to occur as a result of a cyber attack; a number of those interviewed asserted that it just would not be possible.

The human factor

Some degree of complacency on the part of nuclear plant personnel – such as engineers or contractors setting up rogue or unauthorized connections, as described above – may be due to their not being fully cognizant of the cyber security risks. Some of it is also attributable to human nature, which often seeks out shortcuts. Some further examples of poor IT practices at certain nuclear facilities are described below.

Many infection problems stem from **the use of personal devices at nuclear facilities, including directly connecting personal computers to industrial control systems.** This is a problem across industries, as Source 26 confirms: 'Everyone is suffering from BYOD within industrial environments'. In some countries it is common practice to bring personal computers into nuclear facilities, where they provide an avenue for virus infection. Source 6 describes how in some US facilities, engineers regularly bring in their own personal computers in order to run tests and plug them directly into the computer interface of the PLC. For example, in order to assess how a controller is working, an engineer might dock his or her laptop into it and download data on how the device is functioning. If the engineer's personal computer is infected with malware, this will infect the PLC in the process.

> Many computer control systems have PLCs. You can introduce viruses or other malware into a PLC – and we have. Engineers are usually the worst offenders. Often, they will bring their own laptops in, and want to take data off a machine. Lots of times they have introduced viruses in the PLCs when doing tests. (Source 6)

Such actions can have severe consequences. Source 6 cited one well-known example in the industry involving an engineer who inserted a zip drive to download data from a turbine control system (a type of PLC that turns the turbine). However, in the process he introduced a virus into the controller that caused the turbine to overspeed. This, in turn, can cause the reactor to overheat. In this instance, it triggered the fail-safe – but one could imagine a cyber attack in which the fail-safe was compromised.

In some countries it is common practice to bring personal computers into nuclear facilities, where they provide an avenue for virus infection.

Compounding the problem, in some instances **engineers may leave their personal computers unattended in the control room, where they are liable to being accidentally infected** or to infect other devices. Source 6 comments: 'Sometimes engineers will leave their computers sitting in control rooms, I've seen them.' Since running a series of tests can take as long as 10 hours, engineers will exit the control room for certain periods of time but will leave their computers there unattended. (Of course, they will unhook them and shut them down.) But there might be 70 or 80 other people in the control room. 'I've actually seen guys come in, start them up and sign into their email,' Source 6 adds. This of course opens up a pathway for that computer to be infected via a malicious email. In other instances, engineers might have taken data off an industrial control system device and need to upload it to a computer. They will plug in the zip drive that they used to take the data on. At that point, however, if the computer is infected it could infect the USB drive that is used to take data.

The failure to change default passwords is another challenge at nuclear facilities. In some instances, nuclear facilities fail to take basic 'good IT hygiene' security measures, such as changing the factory default passwords on equipment. Manufacturers typically use a simple default password, which is intended to be replaced (Sources 28 and 29). Source 26, too, comments:

> The use of default vendor login details is everywhere, including in nuclear. You just put these in and you can get access to the networks.

While some of these risky situations arise from a lack of rules banning a particular practice, in other instances rules are in place against such an action but the challenge instead is their insufficient enforcement. For example, the use of smartphones is typically not authorized at nuclear facilities. Despite this, Source 27 expressed concerns that engineers might plug their personal smartphones directly into a control system computer in order to charge them; given that these devices lack antivirus software, they are particularly vulnerable.

> If you look at most corporations' policies, they would forbid the introduction of personal mobile devices like smartphones in secure environments. But the problem is they don't enforce it. (Source 27)

Overall, it appears that **while nuclear facility operators are extremely rigorous about enforcing rules that pertain to physical safety and security, they may be less so when it comes to rules that concern cyber security.**

> Operators are really rigid about obeying and enforcing rules. But as rigid as we are about procedures, a lot of the time we are not as rigid about cyber security. One thing operators don't do religiously is have somebody from the IT department check for viruses. And the work requests usually do not require the engineer to run a virus scan on the machine prior to connecting it, either. (Source 6)

> On a standard issue, if we have a procedure that says valves x and y need to be open, we usually send two people to do that and then a third person to check. When it comes to cyber, they'll make sure that the computer is hooked up to the right hub, but they don't have anybody check to make sure that the computer you're hooking up is the one we bought for it and not your own, or that you didn't plug it in anyplace else. They tell you that they do but they don't. (Source 6)

The insider threat

In other instances, the danger might not arise from inadvertent infection but from **deliberately malicious motives.** The 'insider threat' has long been recognized within the nuclear industry as a threat to safety and security and is also a concern from the cyber security perspective. An insider would have the opportunity to insert a USB drive or other removable device into a facility to introduce an infection. According to Source 11, Russian agents have infiltrated nuclear plants in Ukraine:

> I think they have an agent in each plant; it is a priority for them to have people in Ukrainian nuclear plants.

The low wages in Ukraine make workers particularly vulnerable to recruitment by Russian agents, as does the fact that part of the population has loyalties to Russia. Source 11 adds:

> Many government clerks or public employees just want their salary, and they don't want change – the old generation is used to taking bribes, and of course there is a very big lobby for Russian interests.

4. Industry-wide Challenges

Summary

This chapter examines some of the specific challenges currently facing the nuclear industry as it begins to grapple with the cyber security threat. Notwithstanding important recent steps taken by the IAEA to improve cyber security, the nuclear industry currently has less experience in this field than other sectors. This is partly due to the industry's regulatory requirements, which have meant that digital systems were adopted later than in other types of critical infrastructure. Moreover, the industry's long-standing focus on physical protection and safety has meant that while these systems are now relatively robust, less attention has been paid to upgrading cyber security. As a result those seeking to attack nuclear facilities can more easily exploit the weaknesses in digital technology outlined in the previous chapter.

There is increasing evidence that the industry's threat assessment or risk calculation is inadequate, and that it is not investing as much as it should in cyber security, leading to an unbalanced cost–security equation. Developing countries may be particularly at risk, because they have even fewer resources available.

Traditional priorities

The nuclear industry is concerned with both safety and security, and lessons learned from major incidents involving the release of radioactive material have created a culture in which safety is paramount. Although in certain cases safety and security can overlap, there are significant differences between them.

Safety can be broadly viewed as protection against accidental or unintentional incidents. In the nuclear context, the term only includes those incidents that might result in a release of ionizing radiation. The IAEA thus defines safety as the necessary measures to protect people and the environment from accidents that could involve undue radiation hazards.

Security involves protection against malicious or intentional acts. Traditionally, this was rooted in theft protection and physical breach of facilities, although the context has evolved to be much broader, and now includes cyber security. The IAEA defines it as the prevention or response to theft, sabotage, unauthorized access or other malicious acts involving nuclear material or their associated facilities.[6]

The IAEA has now integrated safety and security under the Department of Nuclear Safety and Security that is charged with formulating and implementing the agency's nuclear safety and security programme. The department's activities are aimed at protecting people and the environment from radiation exposure, and it responds to the safety- and security-related needs of its member states.[7]

However, because cyber security concerns only came to the fore in recent years, **the industry has a natural tendency to consider the cyber threat to be relatively low compared with other safety and physical security threats.**

> Within nuclear, safety will always win because, when safety goes wrong, someone gets injured or killed, and with that you get litigation and cost. With security, if you get a security breach, there is a very slim possibility you might get reprimanded or sacked, but it is very unlikely. That is why safety is the prime concern and always will be. (Source 7)

In the aftermath of the 9/11 terrorist attacks on the United States, the nuclear industry invested heavily in physical protection of facilities and materials, with the IAEA promoting major improvements in physical security. In this area, the industry has now reached a high level of security (referred to as 'gates, guards and guns'). However, **this very robustness may in itself make the cyber route a particularly attractive alternative for those seeking to cause damage,** as it is now seen as the 'soft underbelly' of the industry.

Less cyber security experience

The nuclear industry's late adoption of digital systems has resulted in a **lower level of cyber security experience than in other industries**. There were several reasons for this delay. The very high costs of running nuclear power plants mean that equipment used in nuclear facilities tends to be kept in service for at least 20–30 years, while those in other, less costly industries might be replaced every 15 years. Furthermore, the nuclear industry is one of the most heavily regulated in the world, and initial regulatory restrictions prevented the adoption of digital systems. It is only just beginning to address its relative lack of experience of the cyber security challenges associated with digital systems.

> The nuclear industry worldwide is far behind many other industries when it comes to cyber security. Since the nuclear industry was one of the last to start implementing cyber systems due to regulatory reasons, they have among the least amount of experience and expertise. (Source 8)

> There is a safety policy and when you come to any industrial object, you find a lot of leaflets, banners, everything about safety, safety, safety first. But as to cyber security, nobody cares about that. … Remember that all the software or IT systems were designed in order to comply with safety regulations but

[6] IAEA (2014b).
[7] IAEA (2014c).

> not with cyber security regulations. So, in terms of safety, it is definitely bullet-proof, but in terms of cyber security, not so much. (Source 10)

This relative lack of exposure to cyber security issues may also in part explain why a number of nuclear industry personnel do not consider cyber security to be a significant threat.

Limited incident disclosure

While all industries are reluctant to disclose cyber security incidents out of concern for the negative impact on their reputation, the problem is even more pronounced within the nuclear industry. The national security sensitivities surrounding the nuclear sector have fostered an industry culture that is inward-looking and closed, with information typically shared on a 'need to know' basis. **Limited incident disclosure** makes it difficult to assess the true extent of the problem, as nuclear industry personnel might take it to mean that there are very few incidents, reinforcing their belief that cyber security is not a real threat. It also means that the nuclear industry cannot learn from incidents that have already occurred and enhance its cyber defences. Given that a certain cyber attack technique attempted on one plant is likely to be attempted on others, the lack of disclosure means that nuclear facilities do not have warning that they are likely to be targeted by that technique.

> All of the examples in an IAEA training course that I give are the same two or three instances from 2003 and 2008 at a few plants. It looks like we are picking on these plants, but it is just that they are the only ones that have ever disclosed breaches and, therefore, that we can talk about. I am sure that there have been many more. (Source 3)

While only a few cyber attacks on nuclear facilities have been made public, one estimate (Source 8) puts the number of major incidents that have affected industrial control systems as high as 50 (this is in addition to frequent routine attacks on business networks):

> What people keep saying is 'wait until something big happens, then we'll take it seriously'. But the problem is that we have already had a lot of very big things happen. There have probably been about 50 actual control systems cyber incidents in the nuclear industry so far, but only two or three have been made public.

Moreover, some incidents at nuclear facilities are not correctly identified as having been caused by a cyber attack. In some cases, the facility may know there has been a malfunction but not be able to determine the cause. The lack of adequate cyber forensics or logging for industrial control system networks makes it even more difficult to determine the cause of an incident. In other cases, a nuclear facility might not know it has experienced an attack: a hacker could have gained access to the business network or even industrial control system network, but leave no trace. He or she might even be able to introduce a logic bomb, or malicious code that goes undetected until certain conditions are met.

> When things start to go wrong, you might not know it is a cyber attack. (Source 13)

Even when incidents are correctly identified, most countries have few legal requirements to disclose cyber security incidents at nuclear facilities. Since many incidents have never violated an IT security policy, either because they are not strictly an IT issue or because they did not cause an outage, there is no obligation for the facilities to disclose them to the relevant authorities.

The nuclear industry's emphasis on safety at the expense of security may also go some way towards explaining why there is even less disclosure in the nuclear industry than elsewhere: a cyber security breach does not receive widespread attention unless it causes a safety problem.

> When it comes to breaches, if it were a nuclear safety issue, it would be public for sure. But because it is a nuclear security issue, no one talks about it. (Source 3)

Limited collaboration and information-sharing

Another consequence of the industry's 'need to know' mindset is that it is **reluctant to collaborate and share information with other industries** in order to address cyber security challenges. Unfortunately, this means that it is unable to learn from industries that have more experience in dealing with these problems.

> The nuclear industry has always been insular, and the feeling is that when it comes to nuclear, they know best. When it comes to cyber, they do not, period. The bulk of the expertise, the bulk of the experience, the bulk of everything else comes from outside nuclear, but they refuse to use it. (Source 8)

Indeed, the cyber security challenges involving industrial control systems are not industry-specific: the same systems are used in a wide variety of industries, including closely related industries such as the energy and utilities sectors, and thus the vulnerabilities are common to all.

> The information about a problem, for example with a Siemens system, like what happened with Stuxnet, affects every single industry everywhere that uses that same Siemens system. The fact that Stuxnet went after centrifuges … was just the internal programming: what made it cyber vulnerable made it cyber vulnerable to every nuclear plant, fossil plant, water plant, railroad, you name it. This is the exact same Siemens controller, the exact same hard-coded default password that is in every single industry worldwide. (Source 8)

The lack of information-sharing also means that the industry cannot benefit from the use of collective data to identify patterns that can aid attribution (which, in turn, can reveal valuable clues about the intent of the attacker).

At the international level, too, countries are cautious about sharing threat information with each other, as governments are reluctant to share this type of information with one another out of concern that it could be used against them.

Insufficient cyber investment

Another challenge is that there is **insufficient spending on cyber security** within the nuclear industry as a whole. Since owner-operators and vendors tend to focus on profitability and return on investment, they may not be spending enough on cyber security. This, too, is a likely consequence of not thinking that the cyber security challenge is 'real': since the probability of a major attack is considered to be low, such expenditure is not considered a priority.

Owner-operators of nuclear facilities are under constant pressure to reduce the high costs of running the plant. According to Source 5:

> Nuclear facilities are driven by the need to give return on investment.

Source 6 also comments:

> Nuclear facilities are always trying to cut to the bare minimum, simply because it costs so much money to operate. They will always deny that and say they are working smarter, but that is not true.

For this reason, owner-operators are increasingly purchasing commercial off-the-shelf products from vendors because they are cheaper than bespoke products, despite being more vulnerable to cyber attack. In fact, there is a fundamental tension between cyber security and business efficiency. For example, increasing the interoperability of control systems makes them more efficient. But it also makes them more vulnerable since many people have similar devices; someone who can hack into one may be able to hack into all.

Given the other issues they must contend with – safety-related concerns, for example, or physical security challenges – it is not surprising that owner-operators typically do not see cyber security as a spending priority.

> The owner-operators are not terribly interested in spending money on [cyber] security, such as upgrading or replacing existing process control systems. They have got enough things that they want to do without including [cyber] security. It is not something that gets you more production, more efficiency. (Source 13)

Vendors too are not investing sufficiently in cyber security and are making no efforts to design it in from the beginning in future generations of products. Much of this lack of enthusiasm is a problem related to return on investment. A vicious circle is set up: since the owner-operators are not demanding greater protection in this area, vendors do not see a need to spend money to provide it. If there was demand for it, vendors would view it as profitable and would want to build it in.

> The owner-operators aren't pushing the vendors for greater cyber security. This allows the owner-operators to say, 'Well, we can't buy it; the vendors don't make it.' And the vendors can say, 'Well, there is no market demand.' And so everyone is happy doing nothing. (Source 13)

Furthermore, many vendors do not view developing patches as a priority. It is a costly process, and, again, since many owner-operators do not install patches, vendors do not always think it worth their time to develop them. When researchers find zero-day vulnerabilities in their products, some vendors do not engage with them to develop and issue patches for them before researchers make them public.

> Some of the vendors don't recognize that cyber security is even an issue. They're not even responsive to researchers who find vulnerabilities in their products. You would think they would want to develop a patch and get it out to their customers before the researcher tells people about it. (Source 3)

In fact, a profit-driven model may not be suitable for ensuring cyber security in the nuclear industry; **the cost–security equation may be out of balance.**

> The fundamental dilemma is between either building everything bespoke out of components that one can trust, or using the components that are commercially available at a sensible price. The question is, can you trust a 'profit and return on investment'-motivated environment to deal with a truly difficult security problem? (Source 5)

Insufficient agency funding

The agencies charged with providing support to the nuclear sector are often under-resourced, making it all the more challenging for them to allocate sufficient funding to cyber security. This **insufficiency of funding for agencies** manifests itself at both the national and international levels. On a national scale, nuclear regulators often lack resources. At the international level, the IAEA – the world's central intergovernmental forum on nuclear issues – has a team that has been working to issue important guidance on cyber security, but it is small relative to the size of the task.

Infrequent communication between vendors and security companies

Another challenge is the **limited communication between vendors and cyber security companies** – yet communication is essential if the latter are to provide adequate protection. Industrial control systems rely on operating systems and communication protocols between devices that are often very poorly documented or else

proprietary to each major vendor, such as Siemens or Honeywell. This is in part because such technologies are considered a national security issue. In other cases these operating systems or communication protocols are obsolete, so only the vendor may still know how it functions. However, if cyber security companies do not know how an operating system or communication protocol has been designed, it is much more difficult to protect it, as Source 25 confirms:

> If you don't know how a system has been designed, it is hard to protect it. We need vendors to tell us how their products work, so that we can figure out how our products can work in accordance with that.

Few regulatory standards

Given that governments are just beginning to grapple with the emerging cyber risk, there is currently an **insufficiency of regulatory standards.** Only a small number of countries have issued standards on cyber security at nuclear facilities.

> In Canada we are one of the first countries that produced a national standard on the cyber security of nuclear facilities, with new national standard N290.7. There are only a handful of national standards. (Source 3)

When countries do issue guidance, the cyber security measures that they recommend may not be rigorous enough. In the United States, the guidance issued by the Nuclear Regulatory Commission (NRC) is not sufficient to protect against the cyber security threat (Source 8). Even if a nuclear facility were to implement all of the measures in the 'Reg Guide' – a guide that helps interpret regulations and gives guidance on how to comply with them – a number of major cyber security vulnerabilities would remain.

> Two years ago I was involved in doing a third-party review of what I consider the most comprehensive cyber assessment done of any commercial facility worldwide, and it was a nuclear plant. We found major cyber security vulnerabilities that weren't being addressed in the Reg Guide. (Source 8)

Today, governments are increasingly moving away from mandatory requirements in favour of *recommendations* – a trend that is mirrored at nuclear facilities as well. This change results in part from lobbying pressure by the nuclear industry, which seeks to avoid the high costs of complying with such regulation. For example, the Nuclear Energy Institute, a lobbying group which represents the nuclear industry's interests to the US government, put in a request in August 2014 to reduce the number of systems in nuclear plants that would have to be included (King, 2014).

In any event, there also appears to be pressure for less regulation to help alleviate regulators' already stretched workloads and ease the strain on their financial resources:

> There is a push on individual responsibility – that is, having individual facilities determine what they are supposed to be doing to protect their assets – because the regulator cannot look after everybody all the time. However, I would like to see the days again where you have to have this or that in place because it is a lot easier, rather than leaving it to me to figure out what the threat is. (Source 7)

Cyber risk assessment

Some of the circumstances discussed – including the historical prioritization of safety and physical security (to the detriment of cyber security) as well as the industry's reluctance to disclose cyber incidents and share information – suggest that the nuclear industry's cyber security risk assessment may be inaccurate and a worrying underestimate. This is particularly the case when combined with the previous chapter's description of misconceptions among a number of nuclear plant personnel – notably, that they may be convinced that nuclear facilities are air gapped, that this air gap protects them, and that a cyber attack could not result in the release of radioactive material.

Developing and economically stressed countries

Developing countries and others with struggling economies – whether as a result of underdevelopment, underinvestment, economic crises or conflict – **may be particularly at risk.** If a non-state armed group, for example, wished to cause widespread international concern, nuclear facilities in more vulnerable countries might be a preferred target. Source 24 comments that:

> Not all countries have the same level of knowledge when it comes to cyber security. Some countries are just starting to learn about the cyber security challenge.

Source 27 agrees, commenting:

> The problem with developing countries is that – just like with SMEs [small and medium-sized enterprises] – they tend not to have the resources to have security-focused IT staff and large organizations of people that can perform network monitoring functions and so on.

Ukraine provides a useful case study. Source 11 states that the sector in Ukraine suffers from a lack of knowledge:

> In Ukraine, personnel working in nuclear plants are not highly trained in IT. Moreover, they have low salaries so their motivation is very low.

The lack of regulation is particularly pronounced in countries that are under economic and conflict stress. For example, in Ukraine there is almost no regulation involving the protection of critical infrastructure.

Source 11 comments:

> The United States has a CERT for industrial control systems. It may not be enough, but there are some processes, people, and organizational structures in place at least. In Ukraine, we still do not have even a basic structure or management commitment to protect against cyber threats.

The problem is exacerbated by lack of government knowledge on protection against cyber threats. Source 11 adds:

> We have an Information Security Authority that is trying to start protecting critical infrastructure, but they know very little. Then there is the security service of Ukraine, but they are not very good with IT security. Neither is the commission on the safety of nuclear plants.

The challenges in Ukraine and other countries, including developing countries, may be aggravated by the lack of English-language skills among their personnel, which often makes it more difficult for them to access the latest information available on cyber security. Source 11 comments:

> Most people in Ukraine's Information Security Authority … are very bad at speaking English. Only [a few] persons in the CERT teams know English; most do not. And so they produce some documents that are very far from modern practice.

5. Cultural Challenges

Summary

This chapter describes a cultural divide between nuclear plant personnel, or OT engineers, and cyber security personnel, or IT engineers. Their different ways of thinking result in different priorities that are incompatible and can lead to frictions. One such consequence is that nuclear plant personnel often do not understand the cyber security procedures. Additionally, the procedures are not always clearly written, so that nuclear plant personnel may not know whom to call in the event of a cyber security incident, and may therefore not interpret the recommendations or requirements in the way intended by the IT engineers. These communication problems are exacerbated by limited interaction, as those responsible for cyber security are not based on-site. Furthermore, cyber security training at nuclear facilities is often inadequate, and the lack of drills means that nuclear plant personnel have no opportunity to practise these procedures.

Another concern expressed by those interviewed is that security at nuclear facilities is reactive rather than proactive. While this might work in other areas, in terms of cyber security, personnel at nuclear facilities might not become aware of a cyber attack until it is already substantially under way. The combination of factors discussed above suggests that nuclear plants may lack preparedness for a large-scale cyber security emergency, in particular if one were to occur after normal working hours.

Conflicting priorities and cultural divides

Nuclear plant personnel, who are primarily OT engineers, and cyber security personnel, who are considered IT engineers, often have conflicting priorities. The OT discipline concerns itself primarily with the operations of a plant – such as the industrial control systems, including the remote management of pumps and valves – whereas IT is primarily concerned with computers and networks. Each group has different priorities and ways of thinking. In many cases, these different frames of reference will clash, leading to conflict between the two camps. They may often not even realize that their approaches are different and that this will inevitably lead to clashes.

Safety versus cyber security. Historically the main priority of OT engineers has been to ensure the safe and efficient running of the plant; but for cyber security personnel (or IT engineers), security has been the priority.

Source 5 describes a recent IAEA meeting in which the OT engineers (also termed 'safety engineers') and the IT engineers (also called 'security engineers') were approaching the discussions from such different perspectives that they could not understand each other:

> The safety engineers wanted the security engineers to add security to a system, but were telling the security engineers, 'You can't touch the rest of the tests. We have done 19 tests. You're the last test, test 20.' They were bent on making sure that the security engineers did not invalidate any of the previous safety tests. They were essentially saying, 'Just make sure it is right for us and don't violate any of the previous tests.'

In reality, it is simply not possible to treat security as a bolt-on extra to safety in this scenario, because the IT engineers cannot introduce security without risking a change that would invalidate the safety case. For example, a valve controller may have a detailed safety case that has been approved by the plant, but with little or no security to protect the device from interference. If the plant decides to add security to this valve controller, doing so may invalidate some of the safety tests that have already been done, or there might even be unexpected incompatibilities between the security system and the safety system. The system might then behave in such a way that it would no longer be safe. This would be especially true if the nuclear plant wanted to connect the valve controller to the network, in order to gain easier access to data generated by the equipment.

> The reason that the security engineers don't understand is that it is not practical, not possible; you cannot defend a system without altering its state. And so when the safety engineers say, 'You can't alter the state,' the security engineers say, 'In that case we can't defend it.' (Source 5)

Availability versus security. OT engineers prioritize maintaining availability (in other words, keeping the plant running continuously), while cyber security personnel (or IT engineers), as discussed above, regard security as their key focus.

Yet it is not always possible to promote availability and security at the same time. For example, 'patching' a system against a known vulnerability might mean that the system will be unavailable during installation and testing (see Chapter 6). Rather than reducing the system's availability, the OT engineers will often prefer not to patch. From an IT engineer's perspective, patching is a way to improve security against the growing number of cyber security threats. On a larger scale, IT engineers could be in a position where, to maintain the security of a facility's systems, they might require a shutdown of the plant in order to eliminate a cyber security threat – which directly conflicts with the needs of OT engineers.

> On one side, nuclear wants availability as key priority. Cyber wants security as key priority. And often they can't cohabit well. That's the real fight. (Source 25)

Unintentional (accidental) versus intentional (malicious).
OT engineers are primarily concerned with preventing accidents and other unintentional acts. This concern derives directly from their focus on safety. By contrast, cyber security personnel (or IT engineers) tend to focus on preventing intentional acts which might harm the plant, namely malicious attacks (although they are also concerned about unintentional events).

OT engineers' long-standing focus on safety and guarding against accidents means that they have developed rigorous methods of statistical analysis. They approach problems by doing a causal fault analysis, which allows them to look at everything that could theoretically go wrong, the probabilities that all possible events might occur, and what the underlying causes could be. This approach is so central to their culture that they expect the IT engineers to show them the same kind of causal analysis. But IT engineers are not trained to approach problems in this way. The need to consider the intentional threat means that there are simply too many potential, unpredictable events for such an analysis to be undertaken. For example, attackers could make use of zero-day vulnerabilities and other attack technologies that have never been seen before, and new threat actors could emerge.

Frictions between nuclear plant (OT) personnel and cyber security (IT) personnel

Given the conflicting goals and mindsets of nuclear plant personnel and cyber security personnel, it is not surprising that at times some degree of animosity manifests itself between the two. Interviews with personnel from both camps have provided useful anecdotes that further illustrate these frictions and explain some of the underlying causes.

Source 8 emphasized that OT engineers' general dislike of IT engineers is a major part of the cyber security challenge:

> The problem is as much cultural and sociological as it is technical. One of the biggest problems we have is that – as in any industry – the operations people dislike IT.

Source 25, an IT engineer, attempted to view the situation from the OT engineers' perspective:

> I can understand why nuclear plant managers don't like us, because they think we are painful. We come in at the end of a procedure that works [and say that all of these cyber security measures must be added]. We add in cyber security in order to protect them, but from their perspective they don't see the benefit.

Part of the problem can be attributed to the belief among some nuclear plant personnel that cyber security does not pose a real threat; they thus tend to regard the cyber security measures imposed on them by IT engineers as a nuisance, rather than as an important contribution to the security of the plant.

Source 6, an OT engineer who worked for over 10 years in two different nuclear plants in the United States, expressed a number of frustrations with IT engineers. He does not trust their qualifications, particularly as they are rarely nuclear engineers, and believes that they do not understand how a nuclear plant functions. He noted:

> I've never been convinced that if we ever implemented the [cyber emergency] procedure, the guy was even qualified. Certainly not qualified to the extent I was, where I had to go through schools. He might be the biggest computer wizard in the world, he had no idea how a nuclear plant worked.

Without this fundamental understanding, in his view, IT engineers cannot understand why stabilizing the reactor is so essential. As a result, many IT engineers would be unhappy if nuclear plant personnel prevented them from working on an IT problem because the nuclear plant personnel first needed to stabilize the reactor; the IT engineers would not understand why it should take priority.

The extent of the mistrust is such that Source 6 expressed doubts about whether he could rely on the IT engineers in the event of an emergency. He suggested that the IT engineers do not have enough of a work ethic, commenting that 'They want to get the job done as fast as possible so that they can go home. They are not 24/7 workers like we are' – the implication being that IT engineers were less likely to be available in an incident occurring outside standard working hours. Unlike nuclear plant personnel, who are accustomed to receiving urgent calls in the middle of the night, the cyber security personnel tasked with responding tend to be corporate middle managers who are not normally required to deal with out-of-hours calls, and it was felt they might not fully appreciate their critical nature.

The same source observed that IT engineers often wish to know the full extent of a problem before making a decision, or in some cases need to seek permission from the appropriate authority in their management structure before taking action – meaning they might not be able to make decisions quickly enough in the event of an incident. Moreover, unlike nuclear plant personnel, cyber security personnel do not have the requirements on fitness for duty (including working-hour limitations and rules governing alcohol consumption before reporting for a shift), so an OT engineer would not know if an IT engineer responding to a cyber incident had been up all night or was unwell.

Source 6 recounted how in the nuclear plants in which he had worked, the IT engineers developed cyber security procedure documents for the nuclear plant personnel that directed them to stop what they were doing in the event of a cyber incident, to touch nothing, and to call in the cyber security personnel. They did not explain to the nuclear plant personnel the nature of the cyber security risks, how to deal with them, or the rationale behind the procedures:

> The safety of the reactor was always firmly my responsibility. For all the other procedures, for example, if there was a problem with a feed pump, the person in charge fully understood every step and why they were doing it. The reason for that is, in case you got to that step and there was a problem with the equipment, you could devise a solution. So the stuff about 'Stop what you're doing, don't touch any critical control systems' [is surprising].

In addition to the tone being perceived as somewhat offensive by nuclear plant personnel, one problem with such an approach is that in some cases it may be clear that an incident has occurred but the source – whether due to a cyber security incident or otherwise – may be unknown. Therefore, nuclear plant personnel cannot know whether they should call in the cyber security personnel, and the limited information they receive on dealing with cyber security incidents will make it harder for them to diagnose the cause.

Unclear procedures

The interviews also revealed that **nuclear plant personnel often do not understand the cyber security procedures, including those to follow in a cyber-related emergency.** Even the most experienced nuclear plant personnel reported difficulty in understanding the procedures as communicated in the documentation.

> The procedures are confusing as hell … I didn't really understand the procedures. What I knew is that if a cyber incident happened, the first step was that I was supposed to tell the operators to stop what they are doing and not touch any critical control systems. And then the second step, after informing security, was that I was supposed to call whomever the cyber person on call was. (Source 6)

Often, **this is because the procedures are not clearly written.** Nuclear plant personnel report finding the cyber security procedures so hard to understand that they do not always know whom to call in the event of a cyber security incident. In one case, while the procedures documents provided a flow chart of who among the cyber security personnel should be called in such an event, the chart was unclear. Source 6 added:

> It would be like, 'call the director of engineering, who will call someone else, who will then call someone else'. I had no idea who they were and was never sure who the right guy was, who the cyber expert to call was.

In fact, the difficulty understanding the procedures is not limited to OT engineers. The **physical security personnel at nuclear plants,** who must implement IT requirements at times, also **have difficulty understanding cyber security procedures.** Source 7 commented:

> What is frustrating for the [nuclear] security professional is that some of the recommendations are badly written, unclear, and just don't make any sense. Sometimes it is hard to understand what the recommendations are.

Given that the procedures documents were written by IT engineers, with their very different approach and ways of thinking, this is hardly surprising. The nuclear plant personnel's difficulties in understanding the documents are a clear manifestation of the cultural divide. As Source 8 explains, 'One reason the guidelines are unclear is that they were written from an IT security perspective.'

The consequence of this is that the **interpretation of recommendations or requirements by nuclear plant personnel may be very different from that intended by the IT engineers.** OT and IT engineers literally often take different meanings from the same phrase. For example, for OT engineers a 'denial of service' might mean that a 10,000 horsepower main coolant pump in a nuclear plant has shut down. For IT engineers, a 'denial of service' occurs when a malicious flood of data makes a computing resource unavailable.

As another example, although the cyber security procedures instruct nuclear plant personnel not to touch any 'critical control systems' in the event of an incident, it does not detail which system or systems should be regarded as critical. Nuclear plant personnel are thus expected to use their discretion, and their conclusions may be very different from those envisaged by the authors of the cyber security procedures.

Similarly, physical security personnel at nuclear plants might interpret the phrase 'intrusion detection system' as a gate monitor or a card reader. To an IT engineer, an 'intrusion detection system' monitors a network for suspicious traffic.

> The security professional and the IT professional will have a different interpretation of what exactly IT security compliance means; a security professional and an IT professional may have different views on what a control actually is because the documents are badly written. (Source 7)

Another consequence of the cultural divide is that **personnel at nuclear facilities often have difficulty determining what their critical cyber assets are.** For example, in one plant, one of the most critical controllers – the pumps that are used to bring water back into the plant after a loss of feed water event – had its push button located in the highly secure control room but its PLC was in a building that required key card access but was not a vital area. In the United States, there have been some promising recent initiatives to encourage nuclear plant personnel to work with cyber security personnel in order to agree on which assets are cyber critical and need to be prioritized for protection, but more such efforts are needed.

Limited interaction

These communication problems between nuclear plant personnel and cyber security personnel are magnified by the limited interaction between the two. A significant part of the challenge is that **those responsible for cyber security at nuclear facilities are not based on-site** and in fact are often located some distance away; there are thus limited opportunities for the nuclear plant and cyber security personnel to interact in person. Moreover, among the latter, responsibility is often highly dispersed. Thus for most nuclear plant personnel their main contact with the IT engineers is when they come out to the plant on occasion to make repairs. However, these would be unlikely to be the same people who would be responding to a cyber incident.

> No plants in the country have cyber expertise on site. I think that it's all corporate people and that they are not even around. I had no idea who they were. I just knew that they worked in an office that was maybe 100 miles away. (Source 6)

Training issues

It appears that **the level and quality of cyber security training at nuclear facilities are often low compared with the mandatory training for nuclear personnel in other areas.** In particular, some organizations undertaking the training may not have sufficient expertise to do so. Source 23 commented:

> Many companies propose training sessions, but not all of them are equally rigorous. The right people are not always doing the training. Many companies and foundations take norms and say that they can train people, without there being any accreditation process.

Source 6 commented that his training consisted of watching a film (which was not particularly informative) once a year, reading the cyber security procedures documents, and taking an exam based on these procedures. As such, the training also did not address what was happening from a cyber security perspective or how to coordinate with the cyber security personnel. This inadequacy of training is very likely to stem from the nuclear industry's perception that cyber threats are not a high risk.

In particular, the **lack of drills** is a problem since there is no opportunity for nuclear personnel to practise cyber security incident procedures. By contrast, nuclear facilities have regular drills for other scenarios, including integrated drills with the physical security personnel to prepare for the event of an attemped invasion.

The inadequacy of the training is such that when nuclear plant personnel are tested on the cyber security procedures, they may not understand the questions properly and often fail, whereas they obtain high scores in the frequent tests they must take on other procedures.

A reactive rather than proactive approach

Another concern is that **cyber security at nuclear facilities is reactive rather than proactive;** in other words, the focus is on reacting and responding to incidents as they arise, rather than proactively seeking to prevent attacks. In general, defences at nuclear facilities (e.g. physical security) rely on receiving warnings of an imminent attack. For example, if a plane were heading towards a nuclear facility located in the United States, the Federal Aviation Administration would call the facility to alert personnel there.

> Many procedures for reacting to events at nuclear facilities are based on warnings of either an imminent threat or of an event that has occurred … It's all reactive, based on somebody in the plant seeing that something has happened. (Source 6)

> We're reactive to a large extent, something happens in the industry and we learn from it. I can assure you that what happened in South Korea back in December [2014] is going to cause a lot of changes in the way operators and states think of cyber security. (Source 3)

When it comes to a cyber attack, however, there are no such warning mechanisms in place. In fact, as discussed above, **a nuclear facility might not know of a cyber attack until it is already substantially under way.** For example, a hacker could introduce a logic bomb that lies dormant until it is activated to cause physical damage. In the case of the Natanz and Bushehr nuclear facilities in Iran, the nuclear plant personnel knew that their centrifuges were breaking apart. However, it was only months later that they realized that the Stuxnet worm was the cause. In addition, the ease with which malicious code can be hidden makes implementing such a warning system more difficult than in other domains, and in some cases it may be impossible.

Lack of preparedness for a large-scale cyber security emergency

The combination of factors discussed above suggests that **nuclear plants lack preparedness for a large-scale cyber security emergency,** and there would be considerable problems in trying to coordinate an adequate response.

A large-scale cyber security emergency occurring at night could be particularly dangerous. The most confusing time for a system to go out of service is during this time. Of course, there might be an on-call team doing virus scans or other diagnostics, but these are only basic measures, and as Source 6 explained:

> When we have to call people in the middle of the night for other issues that are just as important, like a pump breaking, the response can be slow. If you're calling people at 1 am, it takes them a few minutes to wake up. And say you have 10 people who need to be on the call. By the time you get everyone to dial in, it can take over an hour.

6. Technical Challenges

Summary

This chapter assesses some of the technical challenges involved in providing cyber security at nuclear facilities. Above all, early designs of nuclear facilities – before cyber attacks were a concern – means that they are insecure by design, lacking basic safeguards including authentication and encryption. This means that cyber security at nuclear facilities depends in large part on the successful defence of the network perimeter – all the more so because the flexibility of code means that any attacker who can get past the perimeter defences would be able to make logic changes in the code that are almost impossible to observe. Furthermore, some cyber security techniques such as patching that are standard in home or office IT environments are difficult to implement within nuclear facilities. Lastly, it is extremely difficult to guarantee the integrity of the supply chain.

'Insecure by design'

A major challenge for the nuclear industry, as for most critical infrastructure, is that **cyber security measures were not designed into industrial control systems from the beginning.** The control systems in most nuclear facilities were developed in the 1960s or 1970s when computing was in its infancy and designers gave no thought to the possibility that an actor with a malicious agenda might deliberately try to attack a computer system using electronic means. Against this background, systems were not designed and built with protection against cyber attack in mind, and 'retrofitting' cyber security measures to these original systems now is technically challenging and expensive. Source 3 observed:

> A couple of minor tweaks in how you think about a system right at the very beginning can have huge implications for its security. If security wasn't built in at conception, it is difficult to bolt on after the fact. Actually, it is going to require a redesign.

One example of the 'insecure by design' nature of industrial control systems is the **lack of authentication and verification.** That is, field devices do not require authentication that a command sent to them is a valid command, or verification that it comes from a legitimate source. They are designed to do what they are told without question. This means that any attacker who is able to gain access can just send a command to the device and it will comply. As a result, industrial control systems are particularly vulnerable to man-in-the-middle attacks that alter the communication between two devices:

> The field devices accept the message immediately, without asking. The receiving device does not have to authenticate. Control systems are thus very fragile due to man-in-the-middle attacks. (Source 29)

> You can tell the field device to do whatever you want and it will just say, 'OK, you command, I'll do it.' … The most skilled attackers won't even bother with finding vulnerabilities, they'll use features instead. (Source 13)

Furthermore, **the flexibility of code means that an attacker can change the logic,** or the set of programming instructions, for a piece of equipment in order to cause it to behave differently. This was exploited by the Stuxnet worm. Logic changes are difficult to detect and are therefore a major concern. While it would be technically feasible to examine the code to determine whether any lines had been changed, in practical terms the task would be immense because a typical system could contain billions of lines of code.

This difficulty is exacerbated by the lack of cyber forensics for control systems. For example, they do not generally have log files that maintain records of which parts of the system have been accessed, who accessed them, which information was viewed, and at what date and time. Without a log, it is much more difficult for cyber specialists to determine whether a hacker has gained access or changed anything in the code.

A major implication of the existence of 'insecure by design' systems at a nuclear facility is that such systems rely entirely on network perimeter defence to protect them from attack. If a hacker is able to breach the network perimeter, then the lack of authentication and the flexibility of code provide a number of opportunities to inflict significant damage on the facility.

> It is almost impossible to protect the system once someone gains access to it. That means that right now, we're entirely reliant on the perimeter to stop hackers. (Source 13)

Patching difficulties

The unique aspects of industrial environments (and particularly nuclear facilities) mean that **standard cyber security measures used in everyday home or office IT environments are not necessarily applicable.** Cyber security experts urge home and office users to install patches that will address vulnerabilities discovered in software. Yet patching at nuclear plants presents unique challenges, and is therefore infrequently used.

> Patching is really challenging, and the reality is that very few people are actually installing any patches. (Source 3)

First, unlike in everyday home and office IT environments, patches are less likely to be available for the systems being used. Since these are predominantly legacy systems kept in service for at least 20–30 years, unlike those in home or office environments, many are no longer supported by the vendor. A number of facilities have very old MS-DOS or Windows NT operating systems, for which Microsoft no longer issues patches (or at least, not at a reasonable cost). In some instances the vendor may no longer be in business.

Furthermore, patches risk breaking the system that they are trying to protect. A patch may not be compatible with other software or hardware on a system, thereby causing the entire system to malfunction, or it might have unintended and unforeseen effects. Since the utmost priority is maintaining the availability of the plant, and a patch which does not perform as expected could take an entire plant offline, some operators consider the risk of patching to be too high. Source 3 noted: 'I've seen patches break systems, where they actually disable the system.' In home and office environments the consequences are much less severe and can usually be corrected fairly quickly.

Since the utmost priority is maintaining the availability of the plant, and a patch which does not perform as expected could take an entire plant offline, some operators consider the risk of patching to be too high.

Even if a patch has been approved for software that runs on a vendor's equipment, this does not necessarily guarantee that it is safe to install. The mere presence of one additional piece of software, such as a plug-in, running on a system in a nuclear facility can create an incompatibility with the patch and break the system. The vendor will have tested that the patch is safe in several standard cases, but cannot possibly test every combination of software that a nuclear facility might be running.

> Just because your automation vendor has certified a patch, you don't know whether, because you've got that system with some other plug-in, it's going to have a negative impact. (Source 26)

The unique characteristics of industrial environments like nuclear facilities mean that even patching a facility's commercial network could have significant consequences. It might be reasonable to assume that a facility's commercial network is an 'everyday' office IT environment and that a patching problem there would only affect that network. Yet its interconnectedness with the industrial control systems means that a problem with a patch could affect both systems. As noted in Box 1, at the Hatch nuclear plant in Georgia in 2008, a patch was applied to the business network in order to synchronize it with the industrial control system network. Unfortunately, it introduced incorrect data onto an industrial control system, triggering an automatic plant shutdown.

Owing to the risk of a patch breaking a system, nuclear facilities, again unlike everyday home and office IT environments, must test patches extensively and intensively before they can install them. Patches that affect key systems cannot be applied and tested on the system directly without the risk of taking an entire plant offline. Instead, nuclear facilities often need to set up a costly partial or complete duplicate system to serve as a test bed.[8]

> Having a duplicate system is enormously expensive. And even then, you'll never literally have two identical nuclear reactors. Yet, to have absolutely accurate testing, you would need literally the exact same thing twice. (Source 9)

Even if a patch is available and has been tested, finding a time window in which to apply it is often difficult. Nuclear facilities operate 24 hours a day, but the plant would need to be shut down in order to apply patches, especially if they affect key systems. Some systems provide such essential capability for the running of the facility that even taking them temporarily out of service would compromise the plant's safe operation. Nuclear power plants might typically shut down for maintenance every two years, so installing a patch may not be possible until a scheduled shutdown occurs. Again, this is in contrast to everyday home and office IT environments, where patches can easily be installed during downtime.

> You have to be assured that you have even got a change window. Now, if you have a change window, then potentially the organizations themselves have to take a break from operations, and you are talking about a 24/7 operation. (Source 26)

> Operators are not going to be willing to shut a unit down for three days to install a patch for a vulnerability that somebody might or might not exploit. (Source 3)

Since patching changes the configuration of a system, in a nuclear plant it also makes it harder to monitor the system for unusual behaviour that might indicate infection by malware. Among nuclear operators, the instinct is to avoid making changes to a system so that the operator can acquire a deep understanding of how that system works; the moment a patch is installed, however, the system has changed and the operator no longer has the same depth of understanding of its behaviour. Patching would thus considerably reduce the effectiveness of monitoring techniques, which look for behavioural anomalies. Yet again, this is in marked contrast to changes to the configuration of systems in everyday

[8] Creating a test-bed for a nuclear facility is particularly complex because of the prevalence of legacy systems. Many of the components used at nuclear facilities are no longer manufactured, so operators must try to purchase them on markets for old equipment. Moreover, the equipment must be absolutely identical in order to test a patch properly, since just one difference in a component could cause the duplicate system to react in an entirely different manner. For example, if a computer in a nuclear facility is running Windows 98, then an operator must obtain a Windows 98 computer that has exactly the same graphics card, network card and other elements for the test bed. In procuring components for a test bed, for either legacy or new equipment, part substitutions made by the device manufacturers can present real problems. For example, if an operator buys a personal computer in January and then purchases exactly the same model in March, it is possible that the manufacturer could have changed a small number of components in those three months: even if the two computers are seemingly the same model from the same manufacturer, they may not be identical. Yet even small differences such as these could cause the duplicate system to react in a different manner during testing.

home and office IT environments, which change (and are patched) regularly.

> The default position is that, as you develop and field test a system, that's the way it stays. Industrial operators do that because it works. Every change you make introduces uncertainties and always will. (Source 9)

Finally, patching is a never-ending cycle with new vulnerabilities always being discovered and with them the requirement for new patches.

> You could spend all this time patching your systems and, tomorrow, they will be just as outdated as they were before you patched. (Source 27)

This challenge is magnified by the large number of systems that need to be patched in a nuclear facility. For patching to be effective, an operator could be faced with the requirement to patch every single device in that facility on a regular basis, but there will always be a significant period after the discovery of a vulnerability when a system will be known to be vulnerable while the vendor develops a patch, which then has to be tested. This process could at best take weeks or months, but in many cases it could take years.

> In order to limit your exposure, you need to patch everything. You need to patch your switches, you need to patch your firewalls, you need to patch embedded devices. (Source 27)

It seems, therefore, that each nuclear facility must carefully assess the advantages and disadvantages of patching in each instance. Many appear to have decided that the risks outweigh the benefits and choose not to patch.

Supply chain challenges

Supply chain vulnerabilities are a growing concern since the equipment used at a nuclear facility (and in critical infrastructure more generally) could be compromised at any stage. Backdoor access or exploits could be introduced, for instance, at the vendor's facility, when the equipment is being designed and assembled, or at the locales of any of the subcontractors. For reasons of cost efficiency, vendors are likely to make use of sub-components from other sources, including those produced in other countries. Even the transportation phase is liable to tampering. The Snowden revelations[9] provided evidence that the United States' National Security Agency (NSA) intercepted routers and other network devices being shipped overseas and implanted backdoors, or means of obtaining unauthorized remote access to computer systems (Greenwald, 2014). Source 28 comments:

> We really have no way to defend against supply chain risks in a cyber warfare situation: a computer or system could be compromised in transit or at the place of manufacture.

Although supply chain threats are at present primarily confined to a small number of state actors seeking to prepare the terrain for cyber conflict scenarios, it is possible that terrorist groups or even hackers could adopt such tactics as well.

Of course, intelligence agencies across the world are concerned by these vulnerabilities – particularly in the wake of the Snowden revelations – and a number of countries are increasingly seeking to nationalize their supply chains. However, the reality of globalization is that very few countries are capable of producing all the required parts of a nuclear plant themselves. According to Source 5:

> The US would like to do that [produce all its own components], but I don't think the US can do it anymore. I don't think anybody's in a position to do this.

For instance, just one computer used at a nuclear facility is comprised of thousands of parts. Among these, it is almost inevitable that there might be, say, a tiny chip made in Taiwan, or some other foreign sub-component.

[9] In May 2013 former NSA contractor Edward Snowden leaked tens of thousands of sensitive and classified documents involving US-led surveillance activities.

7. Meeting the Challenges: the Way Forward

Summary

Meeting the challenges described in the previous chapters will require a blend of policy and technical measures. This chapter proposes a series of solutions centred around several key themes. There is above all a need for improved risk assessment guidelines on cyber security at nuclear facilities, which will provide a solid economic underpinning for investment. The 'human factor' can best be handled through a combination of better communication about the risks of poor 'cyber hygiene' and stronger enforcement measures.

Improving disclosure and information-sharing could be achieved by encouraging anonymous sharing, fostering personal contacts at international conferences, and the establishment of industrial CERTs. There is also a need for regulatory standards and more funding for agencies like the IAEA. The cultural divide might be bridged by measures such as encouraging IT engineers to visit nuclear plants, cross-disciplinary educational programmes, and improving cyber security training.

Technical measures such as avoiding the use of non-essential digital features, implementing whitelisting (authorization) technologies, network monitoring, and encouraging the adoption of data diodes can all enhance cyber security. Countries can mitigate supply chain risk by reducing their dependency on foreign components.

Assessing the risk – and attracting investment

Given that many in the nuclear industry do not believe that cyber security poses a real risk to nuclear facilities, a first step is to raise awareness of the challenge. One way to do so would be through the **development of guidelines on ways of measuring cyber security risks in the nuclear industry.** Since at present there is no risk assessment methodology that would permit a nuclear facility to perform a combined safety risk and security risk assessment (only a safety risk assessment and a separate security assessment, which includes cyber security risk), such guidelines include the need for a **combined risk assessment methodology for safety and security.** Developing a methodology will require reflection within the industry, perhaps led by the IAEA's Interface Group, which was formed to address conflicting priorities between safety and security.

A greater understanding of the risk will also help to tackle the challenge of insufficient spending on cyber security in the industry. In addition to **raising awareness of the need to invest in cyber security,** it will **make cyber security more commercially attractive** and provide a clear economic rationale for CEOs and corporate boards to increase expenditure on it.

Since the insurance industry requires solid risk assessments, promoting the further development and adoption of cyber insurance in the nuclear sector might also be beneficial in helping develop these guidelines to measure cyber risk; **cyber insurance may therefore be an important tool to enhance cyber security.** The French government has been conducting a major study on this question. An early conclusion is that to succeed (and to find the right level of underwriters' exposure when measured against the cyber security risk), a key need is the accurate calculation of that risk based on metrics agreed between insurers and the insured.

> What underwriters need is an understanding of the risk and that really comes down to, do organizations have the right people in the right places, with the right authorities, to make the right decisions and have the right policy and operational structures in place? (Source 9)

Insurance may also make cyber security more commercially attractive and drive the process of implementing appropriate measures, by providing the necessary financial incentives (in the form of lower premiums) to persuade owner-operators to invest in them.

> If an insurance company tells an owner-operator that their insurance premium would be very high because they don't have adequate cyber security measures, the owner-operator might just conclude, 'if I spend $100,000 on cyber security measures, I can save $200,000 on the insurance premium'. (Source 10)

Handling the 'human factor'

Given that part of the challenge stems from the 'human factor' – such as engineers or contractors who set up rogue or unauthorized connections or those who plug their home laptops directly into nuclear facility networks – **raising awareness among the personnel involved** of the inherent dangers in doing so will be key.

There is also a need for nuclear facilities to **establish rules where they are not in place already.** For instance, in countries or facilities where personal devices are not already expressly forbidden within nuclear facilities, engineers should be required to hand in any personal devices such as laptops when they enter the facility; the devices should only be returned to the engineers when they depart.

> Engineers should be required to turn in any personal laptops that they bring to the plant. (Source 7)

> If you are going to do any testing and have any kind of device of your own, you should have to turn it in and we will issue it back to you when you bring our laptop back. (Source 6)

There is also a need for rules requiring nuclear plant personnel to **change the default passwords on equipment** to secure passwords; this should apply to both existing equipment and to any new equipment installed.

In order to ensure that engineers actually follow such policies, **enforcement** is key. In particular, independent verification methods, in which multiple personnel check compliance with procedures, should be rigorously followed for cyber security issues. Source 6 suggested that if a device has been signed out, an assigned person should independently check that it is the correct device before it is hooked up to a nuclear plant; a person should also be assigned to run a virus scan on the device.

Technical means can also be used to help enforce compliance. For example, given that nuclear plant personnel may plug USB devices into the nuclear facility computers even though this is not allowed, owner-operators may want to glue USB ports.

> People working in nuclear plants might be more willing to put up with glued ports than they would in a standard IT environment. Glued ports within a plant room probably do not impact productivity; they just make it hard for someone to charge his iPhone. On the other hand, glued USB ports in an IT environment would definitely impact the effectiveness of employees. (Source 26)

Another option is to ensure that USB devices are checked for malware and cleaned before they are allowed into nuclear facilities. One company has developed a technology to do so.

> There is company down in the south of France that has developed technology that provides USB cleaning devices. So we're not saying don't bring your USB to work, but can we at least plug that USB into a special device that will examine all of the data that's on it, it will execute the files that are executable and make sure that there's no malicious software on them before the person plugs that USB stick directly into a critical asset. (Source 26)

Promoting disclosure and information-sharing

Since the industry reluctance to share information about cyber attacks that have occurred stems partly from concern about potential damage to reputation, encouraging nuclear facilities to **share threat information anonymously** would promote greater disclosure. Anonymity could be achieved by asking facilities to **share 'indicators of compromise',** which are traces left on a network or system that indicate a malicious actor has been in the system. These might include phishing emails, the IP addresses from which an attack was launched, or the malware code itself. In sharing indicators of compromise, nuclear facilities do not have to reveal their identity, nor what the impact of the attack has been.

> Sharing indicators of compromise can help the whole industry and improve security. We could anonymously share indicators of compromise without knowing who it was that was breached. (Source 26)

Given that nuclear facilities tend to focus on reacting to attacks as they unfold, another benefit of sharing indicators of compromise is that it would **encourage a proactive approach** to preventing attacks. In communicating valuable information about prevalent attacks – including the types of vulnerabilities exploited by hackers, attack pathways used to gain access, and systems targeted – sharing indicators of compromise would provide others with an early warning of such an attack. This would enable them to put defensive countermeasures in place, perhaps by increasing monitoring or by deciding to patch systems that are identified as particularly vulnerable.

Anonymous sharing has been successful in other fields. As Source 5 commented:

> The airline industry … has set up a platform in which pilots and other industry personnel can anonymously report incidents (for example, if two aircraft come too close to each other); this approach has helped increase disclosure and enhance the safety of the industry.

Such mechanisms could be copied and adapted in the nuclear industry and in the industrial sector more generally.

Fostering personal contacts, which are central for the trust-building required for information-sharing, is also key for promoting the exchange of information at both national and international levels. People may not trust other companies – or governments, for that matter – but they do trust other individuals with whom they have developed strong personal relationships; they are therefore prepared to take the risk of sharing information with them. International conferences can be an important avenue for building these relationships, and more such initiatives in the nuclear industry (and critical infrastructure more broadly) should be encouraged.

> Personal contacts are always best for information-sharing; these trusted environments work best where they co-align common interests of countries or organizations and also personal relationships. (Source 5)

> Conferences where people meet with each other are very important, because when people personally know one another they will not want to attack each other in a cyber warfare scenario. There are not that many nuclear plants in the world, so this should be possible to implement; there needs to be a sense of community. (Source 11)

Although governments are concerned that sharing threat information with other governments could jeopardize national security and thus are reluctant to collaborate at the international level, they recognize that at the national level such sharing is a key priority for defence. Governments can therefore play a key role in encouraging information-sharing within their own countries by **leading the establishment of national Computer Emergency Response Teams specialized in industrial control systems.**

The unique characteristics of industrial control systems mean that CERTs specifically dedicated to industrial control systems will be more effective. In fact, the United States has achieved success with its Industrial Control Systems

CERT (or ICS-CERT) established in 2009, which operates in addition to the national CERT (referred to as US-CERT). Of course, for countries that have yet to establish national CERTs, doing so is a first priority and ICS can be handled as a division within these as a first step.

Regulators need to understand that in order to foster a more proactive cyber security culture in the nuclear sector, they should be content to stay remote from some of the necessary dialogue between stakeholders.

Some measure of government-backed international sharing can also take place between close allies. One avenue for this is the national CERTs; **encouraging greater information-sharing between national CERTs could prove beneficial.** At present, there is only limited information-sharing between CERTs on an informal, ad hoc basis (Sources 19–22). Even though some governments will take more information than they contribute, this will still strengthen cyber security. Many in the industry feel that any information-sharing, however limited, is still better than the current minimal situation.

> It would be helpful to have greater information-sharing between the CERTs. Of course, most countries will want to take information but not give it. But if you allow countries to give what they want and take what they want, it's not ideal, but it's much better than what we have today because today we don't have anything. (Source 25)

Furthermore, given that owner-operators can be wary of disclosing cyber security breaches or incidents in case they are held liable, creating an environment where they feel they can speak candidly without fear of repercussions is key to increasing the level of reporting to ICS-CERTs (or CERTs more generally). The **regulator should reassure owner-operators that they will not be penalized** for any information they share – provided they show good faith – and that, if they disclose a cyber security problem or incident that arose because they violated the code, they will not be prosecuted. According to Source 20: 'To enable information-sharing, you need to develop a culture where whatever you say will not be used against you.'

Regulators thus need to understand that in order to foster a more proactive cyber security culture in the nuclear sector, they should be content to stay remote from some of the necessary dialogue between stakeholders; that their prime focus is on outcomes, rather than on the mechanics of delivering a minimum level of security. They also need to be aware of the difficulties of security in the electronic medium, and take a pragmatic approach to enforcement. Every system, whether it is air gapped, patched or otherwise protected, is liable to intrusion; as long as the root cause of a particular breach is not negligence or purposeful violation of rules, then regulators should only be concerned that the nuclear sector should learn from its experiences as the cyber security culture develops over time and corresponding capabilities are developed.

Developing international policy measures

A number of policy measures would be beneficial as well. Given that only a small number of nations have implemented regulations regarding cyber security at nuclear facilities, the remaining countries should be encouraged to **adopt regulatory standards.** Since a large number of countries follow IAEA guidance, the agency's further development of its work on cyber security at nuclear facilities will prove beneficial. This can be encouraged by **allocating more resources to the IAEA (and other agencies)** to enable them to deal more effectively with cyber security threats.

Particular attention should be dedicated to helping developing countries improve their cyber security readiness in the nuclear sector, given their greater vulnerability. These countries are likely to require funding assistance as well to enable them to achieve this.

Bridging communication gaps

In order to overcome the communication barriers between nuclear plant personnel (OT engineers) and cyber security personnel (IT engineers), **fostering face-to-face communication between the two groups** will be essential. For example, it is important that the cyber security personnel physically visit nuclear facilities on a regular basis. As cost-saving measures, they will be tempted to use methods of remote collaboration, but face-to-face contact is key to promoting mutual understanding between the two cultures. In particular, **encouraging nuclear plant personnel and cyber security personnel to work together on integrated projects** would allow them to gain greater appreciation of each other's ways of thinking. This might involve working together on joint vulnerability analyses or risk assessments, for example. It would also help raise general awareness of cyber security risks among nuclear plant personnel.

> Actually getting the IT guys to work in the plant, to sit with the engineers and work with them, to deploy stuff in OT environments is how you ensure that IT and OT understand each other. (Source 26)

> You need an IT security professional to talk to the on-site security professional so that they can understand the same language. (Source 7)

It will be important to **improve cyber security training at nuclear facilities.** Given that one problem identified is that some of the training may be conducted by groups without sufficient qualifications, there may be a need for **accreditation of training programmes.** Source 24

suggests that the IAEA would be the one vehicle that could provide international accreditation.

In addition, training quality and frequency could be enhanced by **holding integrated drills** on a regular basis. This will also provide an additional avenue for communication between the two groups that will help reduce the cultural divide.

There is also an urgent need for more **cross-disciplinary university and professional programmes.** Interdisciplinary programmes on the cyber security of industrial control systems within the nuclear industry, which include both computer science and engineering disciplines, are now being established, and the creation of more such programmes should be promoted in order to help bridge the cultural gap and start to usher in cultural change within the industry (IAEA, 2014a).

Another initiative to improve communication, in view of the limited dialogue between cyber security companies and vendors, is to **encourage more partnerships between cyber security specialists and vendors.** Deeper knowledge of how vendors' propriety protocols work will enable cyber security companies to provide better security protection for these products. According to Source 25, the cyber security company McAfee has recently signed partnership contracts with vendors such as Alstom and Schneider for this purpose.

Enhancing security

Given that most industrial control systems were designed without considering cyber security requirements – and that, as noted above, it is difficult to 'add on' cyber security at a later date – it is essential that the designers of future generations of control systems take cyber security into account during the initial conception phase. For example, ICS should **avoid the inclusion of non-essential digital features** that could introduce cyber security weaknesses; otherwise, removing such features will require partial or complete redesign. In practical terms this may mean that particularly important functions should not be digitized.

> A couple of minor tweaks in how you think about a system right at the very beginning can have huge implications for the security. If a certain function is particularly important, you might make the decision that you don't even want a computer involved. (Source 3)

Additionally, given that the growing uptake of digital systems is leading to a reduction in redundancy, it is important for nuclear facilities to realize this and to **ensure that sufficient redundancy is retained.** This may involve, for example, making certain that there are manual backups for critical systems in the event of a failure.

Encouraging the greater adoption of authentication and encryption technologies in future generations of ICS will also be key, since their lack contributes to making SCADA systems 'insecure by design'. Adding authentication when sending and receiving communications or commands means that the different parts of a SCADA system have to prove their identity to each other – and that the communication or command being transmitted is legitimate. It makes it harder to carry out cyber attacks that send an unauthorized command to a device that automatically accepts it, or that falsify communications (as happened with Stuxnet, for example). And adding encryption to authentication would also make the contents of the communications or commands unintelligible to hackers, providing an even greater level of security. Source 29 confirms: 'The solutions to the 'insecurity by design' challenge will involve encryption and authentication.'

Given that the unprecedented flexibility of the current generation of ICS also makes them 'insecure by design', it will be vital to restrict their malleability. While the specific nature of industrial environments means they face particular cyber security challenges that do not exist in everyday home or office IT environments – such as patching difficulties – these special characteristics also permit unique cyber security solutions that would not be possible in the latter. **Promoting the adoption of 'whitelisting',** for example, could therefore be an important way to bolster cyber security at nuclear facilities. As an information exchange protocol that only permits actions or traffic if they are on an authorized list known to be safe, whitelisting contrasts with traditional 'blacklisting' methods of cyber defence, a model under which all actions or traffic are permitted unless they are on a blocked list.

Whitelisting can be done both at the device level and at the network level. At a device level, the methodology involves authorizing the device to carry out only a narrow set of actions that are necessary for its role. The computer would only be allowed to run certain types of pre-approved executable files, rather than, as now, any executable files on a USB key. This would reduce the risk of infection carried across an air gap by insertion of a USB device (which was the likely pathway used by Stuxnet).

Whitelisting at a network level involves only authorizing traffic between specific points that are needed for its activities. For example, instead of allowing a computer to talk to all of the computers on the network, whitelisting would only allow it to talk to a small number of other previously identified computers with which it needs to communicate.

Industrial environments are particularly suited to whitelisting because they are predominantly static in functionality, making it possible to determine exactly what actions or traffic should be authorized. Most

everyday home or office IT environments are in constant flux. At the device level, users regularly download new software on their computers – either new applications or software updates to existing applications. At the network level, computers are regularly added to or removed from parent networks. These computers also generate a lot of unfamiliar traffic, as they visit new websites and receive and send numerous emails to and from new people all over the world. This results in a high level of unpredictability.

By contrast, the industrial world is relatively fixed. At the device level, patching is rare (particularly in the nuclear environment), so device configurations change little. At the network level, industrial control systems primarily involve computers talking to computers; thus the communications and commands that different parts of such systems must exchange with other parts should follow relatively stable patterns. This predictability makes it possible to determine what actions and communications should be authorized in industrial environments.

> Within an industrial control system environment, especially a nuclear environment, actually being able to secure these environments is infinitely easier, not harder, than it would be for an IT environment. (Source 26)

Whitelisting can also provide a solution to the patching challenges experienced by nuclear facilities: by restricting the functionality of a device or network, it becomes less important to patch systems, and this in turn facilitates whitelisting.

> If you compare the effort of doing whitelisting with the effort of patching and vulnerability management, they are not even vaguely related in scope. (Source 9)

In order to implement whitelisting, if the programmable logic controllers are modern, purchased within the last 10 years or so, and as long as they are digital, only a firmware upgrade to them or a new ethernet card would be needed. The financial expense of an upgrade would be manageable. In fact, the largest share of the cost would be the additional testing and planning needed to make the upgrade safely.

If a system is older, perhaps 20–30 years old, then whitelisting may not be possible. In this case, other options that can add security include active management, the deployment of intrusion protection systems, and intrusion detection systems which monitor the electronic traffic within a nuclear facility for anomalous behaviour. Some of these are discussed further below.

Intrusion detection systems such as network monitoring, which involves examining the traffic within a nuclear facility for anomalous behaviour, would enable nuclear facilities to take a more proactive approach to cyber security. When the system detects unusual traffic that does not fit the established pattern, it alerts the owner-operator.

For many facilities (nuclear and otherwise), the first step in network monitoring is to map the expected traffic between devices in order to establish a standard baseline. Many nuclear facilities have yet to do this, and others may not have undertaken the mapping at a sufficiently detailed level.

> It is vital that operators identify the devices they have, identify how they communicate with each other, and put in place technical systems that will immediately alert the operators as soon as any of that ever changes. This is typically not done in industrial settings. It is done to a greater degree, but far from ubiquitously, in nuclear. (Source 9)

> Because people are not thinking about security, they are not doing the data flows at the level that is needed for security. The way data flows are currently documented is, for example, that this computer sends data every 10 minutes over to that computer. But what we need to know is the communication between IP addresses or ports and the data format. For example, if a computer is trying to access an IP address outside my company on port 80, that would be a red flag because it is indicative of a backdoor access Trojan sending data back to a command and control server. (Source 3)

The **use of virtualization** – the creation of a virtual version of a device, operating system or network – may be a useful process in helping understand the data flows and serve as an effective way to map out those connections. By virtualizing the entire network, it is possible to learn about the data flows without the degree of risk involved in actual experimentation.

> We can use virtual environments to learn about the data flows without having to experiment with our real network and worrying that we are going to mess it up. (Source 3)

Furthermore, **monitoring needs to be done on the entire industrial control system network, not just on the perimeter.** Since personnel at nuclear facilities (and, in fact, critical infrastructure more generally) too often concentrate only on perimeter defence, allowing malware to operate undetected if it is able to get past the perimeter, they need to recognize that they must monitor *all* networks.

> Most people focus all of their security on prevention and they do very little for detection and containment. Network monitoring tends to be on the perimeter and very little [on] any form of network monitoring within the control system. So people need to monitor all their networks, not only the perimeters. (Source 27)

In addition, encouraging **the adoption of secure optical data diodes** where not already implemented would significantly enhance cyber security. This is key given that there are some nuclear facilities that may have only a firewall to protect the industrial control system network.

With regard to supply chain challenges, the globalization of manufacturing means that resolving vulnerability remains difficult. However, some countries are taking important **steps towards the nationalization of their supply chains** (in the nuclear sector and beyond).

Japan has had the greatest success here in enabling indigenous companies to build the entire product range for its nuclear power plants. Although of course microchips from foreign sources may be used, Source 18 states that Japanese power plants are 'almost 100% national; they make the products that they need'.

The best option for countries that lack the required extensive national industry is to **reduce their supply chain vulnerability** to the maximum extent possible. Russia, for example, views the nationalization of its supply chain as a priority, including in the nuclear sector. Given the difficulty of manufacturing all of its products domestically, in the short term Russia is seeking to reduce its dependency on components manufactured in countries that it considers 'less friendly'; instead, it is substituting them with components from China, which it considers a 'more friendly' country at present. Russia views this as an intermediate step while it continues to build up its own national industry. In the long term, it hopes to be able to replace the majority of components with Russian products.

> Throughout all of last year, there was a big discussion in Russia about the need to urgently replace foreign components and hardware with Russian ones. This attitude extends to all spheres and sectors of the Russian economy. (Source 12)

Of course, for financial reasons it will be important for nuclear facilities to identify the most crucial parts of the plant from a cyber security perspective (notably, their critical cyber assets) in order to grant those the highest levels of protection. As Source 3 states, 'It needs to be a graded approach; we can't afford to do everything for every system.' **Prioritization of the cyber risks is therefore key.**

8. Developing an Organizational Response

Summary

This chapter sets out a series of proposals for the development of a response regime in the civil nuclear industry. This regime would be aimed at mitigating cyber security problems identified above, and at addressing others. It would be based on an organizational methodology that is scalable and flexible, and able to act with confidence and authority, but that would be driven by the overriding need to keep providing nuclear-sourced energy rather than by the sometimes commercially restrictive requirements of the security profession.

The need for organization

In cyber security, organization is a prerequisite for everything. Technological responses on their own have failed. So have data-centric responses. Without organization, communication and cooperative actions involving stakeholders and individuals will always be inefficient and ineffective. Without organization, a strategic cyber response does not work.

Acting coherently, stakeholders involved in a future civil nuclear cyber security regime should have as their goals to turn the components of cyberspace that are key to achieving strategic sectoral aims into a self-governing eco-system, instead of, as now, an ungoverned environment made up of disparate components, each engaged in tactical battles with a variety of threats. The comprehension involved must also reach beyond simply cyber security into physical security, personnel security and safety. In addition, meaningful and persistent dialogue between IT and OT stakeholders must be incorporated as a fundamental necessity.

Cyber security is a multi-dimensional concept that cannot readily be accommodated within traditional security policy-making. In the nuclear sector, both safety and physical security measures have developed incrementally and in tandem over time, but the rapidity in the development of cyber dependency creates dissonance within a security regime. Three essential components (physical, virtual and personnel) are evolving at different rates, in terms of both threat manifestation and countervailing capability development. This leads to a twisting complexity in the management of overall security (with additional complications of insider threats posing problems across all areas of risk).

This environment must continue at all times to establish the appropriate balance between regulated and self-determined actions to avoid any tendency towards overall stagnation, which is a condition attractive to organized groups and individuals aiming to challenge the welfare of the nuclear energy supply chain.

Communication

The various illicit uses of cyberspace amount to a system-level challenge to the civil nuclear sector. As it is currently configured, however, the sector does not act and respond as a coherent eco-system where cyber security is concerned. This is despite fifty years' experience of developing a safety-related (and more recently a security-related) culture. Stakeholders in the nuclear cyber domain remain largely segregated, despite having a satisfactory set of enabling computer security policy documents that act as a potential operational glue. As a result, agencies within the sector may well fail to see that they are affected by another stakeholder's cyber security, or, more often, by the lack of it. This is a matter of communication, both horizontally between nuclear energy producers, but also vertically throughout the entire supply chain.

Improved coordination

At a simple level, the priorities for a cyber security regime are nothing but traditional: deterrence, prevention, detection and response. But it is how these activities are coordinated that will set the tone of the nuclear sector's cyber security culture, closely allied by absolute necessity to the safety culture already at the core of the industry.

Hitherto challenges in the cyber domain, no matter in which industrial sector, have been managed generally by a patchwork of technological responses. The nuclear sector is no different from any other. However, there is ample evidence to suggest that the main challenge, affecting the entire sector, requires an equally far-reaching response mechanism to achieve higher overall levels of security, thus providing confidence in the use and maintenance of electronic control and information systems. Without appropriate controls in behaviour, the potential for technology to deliver future efficiencies in the nuclear energy life-cycle will become limited; the threat picture begins to build, but awareness on its own does not act as a catalyst for the technological design of operational and defensive systems, which fail to keep pace with the real world.

In order to attempt to correct this imbalance, cyber security policy within the sector needs to be extended to fuse two approaches: the largely reactive and bottom-up concerns with computer and network security, along with information security and assurance; and the top-down approach driven by the needs of sector-level responsibility to deliver nuclear-sourced energy safely and at commercial prices. If this organizational transformation is achievable, it should be possible to shape future cyber security policy to align with strategic perspectives – primarily the needs of the nuclear business, but also progressive strategies

on governance and regulation, cost-effectiveness and, particularly, inclusiveness.

The term cyber security and other related expressions are widely used as though their meaning were clear and incontrovertible, but the primary research for this report confirms that there is no consistency in approach to cyber issues across the international stage, and the nuclear sector is no exception. The lack of an international cyber lexicon continues to hinder multilateral responses in all sectors, particularly when applied across linguistic barriers. Even within individual states, the interpretation of 'cyber' can mask a range of inconsistencies and unanswered questions, posing a serious difficulty for policy-makers and those tasked with ensuring security. In several languages, for example, there is only a single word for both safety and security.

Even within individual states, the interpretation of 'cyber' can mask a range of inconsistencies and unanswered questions, posing a serious difficulty for policy-makers and those tasked with ensuring security.

One way to achieve alignment across and within all stakeholder groups might be to put one set of stakeholders (such as the technical cadre) at the centre of the problem and then organize the response around it. However, the foundations of a more integrated and robust regime in any sector require a common idea of cyber security – as regards both the problem and responses to it. At the top of the IAEA policy tree there is some very sound advice already being developed, but at the centre of the downstream problem is the lack of a common baseline in building a potential cyber response. This makes development of a unified approach to cyber issues all the more challenging. Creating a common lexicon for cyber security, and hence a common threat picture, as well as acknowledging differences in national cultures in terms of risk management, security vetting and operational responses, are all issues for further and immediate consideration.

Regulation

The threat that the nuclear sector faces in cyberspace is fast-changing, sophisticated and potent, suggesting that a response mechanism needs to be equally powerful and agile. However, meeting an unresponsive and arguably obsolete regulatory requirement being enacted in a highly regulated environment (which is the cultural norm in the nuclear industry) would only be counter-productive. Such an approach would quickly strangle the vitality of a potential response based on the mature culture that the nuclear sector enjoys in the matter of safety. Instead, there needs to be a well-judged and informed balance in policy, regulation and communication. A potential solution would be to support regulatory authorities with accredited specialist cyber security expertise that can act with appropriate agility and speed.

A strategy that shifts the risk of cyber-related harm to proactive rather than reactive measures would serve to deter cyber adversaries by increasing the degree of difficulty they will encounter if attacking the sector. This approach would deflect threats to easier targets, while also ensuring that any determined adversaries would have to invest more to achieve their aims. A nuclear-cyber security regime needs to be put in place to make the sector hostile to saboteurs, while maintaining the delicate balance between prescriptive regulation and the empowerment of knowledgeable people to take appropriate mitigating action where necessary.

This approach would need to be high on vision, doctrine and knowledge, and moderate on control. The development of cyberspace with its embedded insecurities will always outpace any internationalized hierarchical structure designed for policy development rather than operational response. Such a regime would allow the fullest of freedoms to those who have a role to play in countering risks to the security of the sector, while also contributing to a broader approach to cyber security through a policy of inclusiveness. It will rely to a much greater extent on creating a shared awareness of cyberspace, its threats and operating methods, as well as the spectrum of available security capabilities, including collective protection, to mitigate risk.

Technological responses

Such a security regime would have to incorporate a technical response to address the issues described earlier (such as patching or air gapping). This would fit into an organizational approach to risk reduction, which can be bought into action rapidly and uniformly to raise the level of security to address critical vulnerabilities across the sector. Thus an appropriate overall response would comprise an eco-system in which the activities of different responding agencies and bodies complement one another and are mutually reinforcing, rather than conflicting; this would include a very close cooperation with the safety cadre and the physical security teams on sites. An approach to cyber security that draws in a wide range of people from across the sector and also further afield (national regulatory bodies, for example), scarcely lends itself to centralized control. Cyber security operations at nuclear facilities therefore need to be self-informed, self-governing and spontaneous, but to act within an agreed framework that is coordinated more centrally, most probably by the IAEA.

There is limited evidence of cyber attacks on the civil nuclear sector, most likely owing to lack of disclosure (as is common in other reputation-sensitive sectors such as finance, but also perhaps from a lack of discovery. Current responses to the exploitation of cyberspace by adversaries characteristically lack both agility and organization, making it difficult to improve security systematically and efficiently. Organized threats require organized responses by the whole sector, which necessarily includes leadership at the highest level (supported by up-to-date advisory bodies) with energetic and knowledgeable inputs from the various internal and external stakeholders. Technological capability involved in protection, detection and response capability needs proportionate investment, gearing to risk registers and recognition of the guidance and recommendations for cyber security that the IAEA is developing on behalf of its member states.

Governance

The governance of cyber security in the sector has to be able to promote debate around two key factors. First, responses need to be managed in a way that creates a norm that supports the use of information and communications technology (ICT) to ensure safe and efficient nuclear energy production, while increasing the difficulties for threat actors.

Second, cyber security management must have a collective dimension, involving all the key stakeholders and organizations. Clearly, where vulnerabilities remain in infrastructure protection or information assurance, these are likely to be discovered (whether by accident or design) and exploited by the ill-disposed. A collective approach would enable cyber security to become a self-taught, dynamic process based on common operating principles to counter evolving threats, and benefiting from a doctrinal loop based on the 'Boyd cycle' of continual process improvement (observe, orientate, decide, act). If each stakeholder were to be given the opportunity to learn from the experience of others, the overall level of cyber security across a chosen sector should increase (and has been demonstrated to do so in the UK financial services through concepts such as the virtual task force (Home Office, 2010)).

Effective and durable responses in cyberspace therefore require a shared awareness, an appetite for collaboration and the development of an instinct for risk, which might alternatively be described as a culture of cyber security. But achievement of this relies once again on developing a truly knowledgeable leadership at the very top of the eco-system, and then within its subsections too.

Risk management

To achieve absolute security in cyberspace would require all threats, their toolsets and their attack paths to be identified and isolated, and certain interactions to be interdicted before they became critically dangerous.

However, taking into account the complexity of the internet, the rapidity with which malware is developed and the unpredictability of the human component of the environment, such perfect security is a fantasy – and perhaps not even a desirable one at that, given the constraints that would place on the industrial processes involved.

Thus the requirement for a civil nuclear cyber security regime must be to manage and mitigate rather than eliminate threats from cyberspace and to assess these threats relative to vulnerabilities, the likelihood of an attack and the potential impacts if an attack is successful. Cyber security therefore becomes a matter of risk management, within an environment in which the key element of the responsive entity is the development of pace and agility.

Inclusiveness

A technological approach alone will not be sufficient to resolve the complexity of the security space. An approach to cyber security which is entirely or largely technological will lack depth and deny the defender the ability to develop an interlinked series of layers of security, each representing another hurdle for an attacker to overcome. Understanding the intersection between the technical, human, organizational and regulatory aspects goes to the heart of solving, or even merely mitigating, the problem of cyber security in any sector, let alone the politically sensitive theatre of nuclear energy production

Given the technological sophistication of the cyber medium, the pace of change and the way in which user demand on the internet catalyses high degrees of innovation, security within ICT infrastructures could be seen as just too great a security problem for analysts, industrialists and policy-makers. This condition exists nationally, internationally and within industrial sectors themselves, with complex sets of regulatory authorities trying to make their respective marks on the structure of cyber security within their own ambits. But this does not necessarily have to be the case in the nuclear sector, where there are fewer stakeholders, they are generally acquainted with one another, and the culture of 'collectivism' is more clearly accepted (principally through the traditional lens of 'safety'). This fundamental principle in the delivery of nuclear safety has the potential to extend to a complementary development of cyber security in the sector, given the appropriate push by regulators and the development of a workable model of the response required.

Configuring the future response

Within this difficult concept of cyber security, some capabilities can be identified as simply common sense, aligned to general principles in risk management systems where most resources are expended on the most critical vulnerabilities. However, the philosophy of taking proactive action to mitigate risks when they are identified rather than focusing on responses when they occur – often called 'left-shifting' risk management (Jonas 2011) – also points usefully to the less resource-intensive (and less expensive) preventive activities of education, training and exercising.

The key features of the response will be agility and initiative; and taking both an actor-neutral and a risk-based approach.

Agility and initiative. As described earlier, the range of cyber threats is so broad and the spectrum of threat actors so diverse that a 'line in the sand' cyber defence philosophy will mean two things. First, the agile and intelligent (and well-resourced) cyber adversary, who is unencumbered by long-winded business processes, will enjoy a good deal of initiative in the contest, and will not have to compete particularly vigorously to gain or maintain the initiative. Second (as is borne out by our interviews for this project), the response to cyber threats will tend to be reactive rather than anticipatory, with reaction only occurring when an attack hits the firewall or is detected inside it (if it is detected at all). In other words, the point at which response mechanisms of the sector begin to address cyber threats is when those threats are fully developed and at their most powerful. Before such an event occurs, attacks may even have been rehearsed on other sectors, nationally or internationally, particularly those containing a preponderance of industrial control systems. The nuclear sector's cyber security response should therefore seek to be as agile as possible and should focus on unbalancing an opponent by winning and maintaining the initiative, and where possible activity should be intelligence-led. The intelligence component, which includes horizon scanning, research and development (R&D), and information from other actors in the sector, thus helps to determine the triggers which invoke the response mechanisms.

An actor-neutral approach. An 'actor-neutral' approach in which capability is developed irrespective of particular (and known) threat actors would be preferable, given that these are so diverse and can change quite quickly. What is important is the knowledge of what an adversary (any adversary) could do, and to have the policies, procedures and equipment necessary to meet (or anticipate) that challenge, whatever its origin and whenever it occurs.

A risk-based approach. It would not be reasonable to expect to eliminate all cyber threats permanently, nor would it be possible to filter out all criminal or hostile use (actual or potential) of the global ICT infrastructure. However, a risk-based approach to cyber-security will:

- Indicate that legitimate use of ICT should not be assumed to be free of plausible adverse consequences;
- Enable cyber security to be assessed on the basis of proportionality: perceived benefits can be set against possible penalties, and benefits can therefore be prioritized;
- Encourage agility and adaptability: as cyber security challenges evolve, priorities can be recalibrated;
- Allow cyber security policy to be framed at an overall or system level, with risks and dangers in one sector being offset by benefits and advantages in another.

A cyber security regime

In transforming cyber security management in the direction proposed in this report, it becomes reasonable and useful to describe these efforts as aspects of a sector-level cyber security 'regime'. Such a regime will define a methodology to organize efforts through the national and international development of enabling policy, while acknowledging that successful cyber operations will need to remain delegated to power plants via their commercial parents.

A successful and durable regime is one that functions intelligently and responsively within its area of concern, remaining absolutely current with the threat picture, concomitant risks and the arsenal of available countermeasures.

Any management system that remains centrally driven or over-prescriptive would risk reducing pace and agility in the response, leading to ever-widening capability gaps between threats and responses and thus higher risks. A successful and durable regime is one that functions intelligently and responsively within its area of concern, remaining absolutely current with the threat picture, concomitant risks and the arsenal of available countermeasures. The regime method offers the most suitable basis for a sectoral cyber security strategy because it can include and empower (not direct, as to do so would cause resistance and impose delays) a wide variety of actors, agencies and stakeholders. It can also be sufficiently agile (yet without losing focus) to meet a rapidly evolving and transforming security challenge.

An active strategy for cyber security can thus be developed in a series of steps:

- by establishing an agile organization;
- by articulating a sectoral policy;
- by careful planning and deconfliction; and
- through developing responsiveness.

On the basis of the analysis above, an effective sectoral cyber security management regime would:

- Promote a sectoral-level approach, from the highest levels down to the individual;
- Support a progressive environment which is designed to sustain tempo, and set out to establish the appropriate balance between regulation and the need to foster a culture of organizational and personal responsibility;
- Draw inputs from all available sources of cyber expertise;
- Incorporate a formal and properly funded environment for the promotion and fostering of cyber security within the sector;
- Enable the free flow of information between all stakeholders, creating a knowledgeable group in which the key tenets of leadership, responsibility and accountability can be clearly identified;
- Incorporate the necessary mechanisms to enable in-depth preparation for cyber security challenges, however these may arise, and an agile and coordinated response, including horizon scanning and R&D to extend the boundaries of the regime to the maximum extent possible;
- Define unambiguous communications channels to national and international specialist agencies.

While society at large is becoming more engaged in the cyber security problem, progress in the nuclear sector has been more laboured. Although the IAEA has developed some sound guidance on computer security, hitherto the culture of the sector has remained focused on the issue of safety. This has left the implementation of cyber security largely passive, defensive and uncoordinated; both 'agility' and 'organization' seem in short supply. This has led to considerable inconsistencies in technical implementation.

The organized way in which threats are manifested through the internet requires an organizational response by the civil nuclear sector, which includes, by necessity, knowledgeable leadership at the highest levels, combined with dynamic contributions by management and staff and the entire stakeholder group, including members of the wider security and safety communities. Energetic and knowledgeable inputs from internal communities and individuals and also external agencies such as government bodies will be welcomed by the cyber security regime. Each of these stakeholders has a role to play in a system which must generate 'tempo', be agile, and create an environment in which innovation is allowed to flourish and inefficient processes are challenged.

9. Conclusions

This report has examined the range of cyber security challenges at nuclear facilities and proposed a number of specific solutions to the challenges identified, as well as various actionable recommendations for the nuclear industry on a more general level. (For convenience these are listed at the end of the Executive Summary.)

Perhaps the greatest cyber security issue facing the nuclear industry is that many in the sector do not fully understand the risk, and therefore a key first step is to develop guidelines to assess and measure this risk as accurately as possible. This will help CEOs and company boards to understand what is at stake, and also provide them with a clear economic rationale to invest in cyber security. The development of cyber insurance, with its strong reliance on risk metrics, may be an important tool for promoting the development of cyber risk guidelines. In tackling the challenges related to the 'human factor', it will also be important to raise awareness among both engineers and contractors of the risks involved in setting up unauthorized connections or plugging in personal USBs at nuclear facilities. Measures that promote disclosure and information-sharing can also play an important role in enhancing cyber security, as can regulatory standards and other policy measures, improved communication to bridge cultural divides and the implementation of technical solutions.

The nuclear industry as a whole needs to develop a more robust ambition to take the initiative in cyberspace and to fund the promotion and fostering of a culture of cyber security, determining investment priorities and ensuring that sufficient and sustained funding is allocated to effective responses to the challenge. It also needs to establish an international cyber security risk management strategy and encourage the free flow of information between all stakeholders. This will require the industry to develop appropriate mechanisms and coordinated plans of action to address the technical shortfalls identified, as well as to find the right balance between regulation and personal responsibility.

The report has also highlighted some important areas for future research. Given that developing countries have been found to be particularly vulnerable, their specific needs should be assessed so that resources can be allocated more efficiently to combating the particular risks identified. The apparent lack of preparedness for a large-scale cyber security emergency, particularly one that occurs outside normal working hours, also suggests that scenario-based planning studies and exercises would lead to a better understanding of how a situation might unfold in a crisis – and to the development of effective response plans across the industry.

A number of the findings in this report may have a wider relevance, beyond the nuclear sector, since many of the challenges described here are common to critical infrastructure more generally. Examples of solutions that could apply across all sectors are initiatives to bridge communication gaps, the adoption of whitelisting techniques and the creation of industrial CERTs.

The main purpose of this research initiative has been to contribute practical and valuable ideas for decision-makers in the spirit of increasing safety and security in the nuclear industry. We hope that the findings and conclusions will stimulate lively discussion in the nuclear sector about the risks of – and responses to – a wide range of potential cyber attacks, thus benefiting the industry as a whole and the societies that it serves.

Annex: Interview Sources

Those interviewed for this report (identified in the report by number) included the following:

1. A UK-based director at a major international company specializing in cyber security
2. A UK-based technical expert at a major international company specializing in cyber security
3. A senior technical officer working on control computers at a Canadian owner-operator of nuclear power plants
4. An expert in the cyber security programme of a major international organization dealing with nuclear security
5. A consultant to the IAEA
6. A recently retired operations shift manager at a US nuclear power plant (with experience in two different nuclear power plants in two different parts of the country)
7. A recently retired UK Civil Nuclear Constabulary (CNC) security manager at a UK nuclear power plant
8. A US industrial control systems expert who was trained as a nuclear engineer
9. An industrial control systems expert at a US public-private centre for knowledge-sharing on industrial control systems cyber security
10. A UK-based director at a major international company specializing in cyber security
11. A Ukrainian expert on cyber security who was trained as a physicist
12. A researcher working on cyber and nuclear security at a Russian think-tank
13. The CEO of a US-based company specializing in cyber security
14. A cyber security expert who had worked on nuclear security at a Japanese think-tank
15. The chief technology officer of a division providing defence-related products at a large Japanese multinational technology company
16. The manager of a centre dealing with the security of control systems at a Japanese vendor to nuclear power plants
17. A security systems researcher at a Japanese industry research laboratory
18. The chief cyber security engineer at a Japanese vendor to nuclear power plants
19. An expert on network and information security at a major EU agency dealing with cyber security
20. An expert on CERTs at a major EU agency dealing with cyber security
21. An expert on ICS-SCADA systems at a major EU agency dealing with cyber security
22. The head of the resilience and critical information infrastructure protection division at a major EU agency dealing with cyber security
23. A director at a French owner-operator of nuclear power plants
24. The director responsible for cyber security at a French owner-operator of nuclear power plants
25. A France-based director at a major international company specializing in cyber security
26. A UK-based vice president and chief technology officer at a major international company specializing in cyber security
27. An expert on SCADA and other industrial control systems who founded an online information platform
28. A senior expert on defence and security at the French Ministry of Ecology, Sustainable Development and Energy
29. A senior expert on nuclear security at the French Ministry of Ecology, Sustainable Development and Energy
30. A German cyber security expert providing consulting services to nuclear power plants

References and Select Bibliography

Anderson, Nate (2012), 'Confirmed: US and Israel created Stuxnet, lost control of it', *Ars technica*, 1 June. http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.

BBC (2011), 'Facebook and other social media "used for cyber jihad"', BBC News, 12 July. http://www.bbc.co.uk/news/uk-politics-14126514.

Boulanin, Vincent and Ogilvie-White, Tanya (2014), 'Cyber Threats and Nuclear Dangers', *Policy Brief* 17, November (Canberra: APLN (Asia Pacific Leadership Network for Nuclear Non-Proliferation and Disarmament) and CNND (Centre for Nuclear Non-Proliferation and Disarmament)). http://www.a-pln.org/sites/default/files/apln-analysis-docs/Policy%20Brief%20No%2017%20-%20Cyber%20Threats%20and%20Nuclear%20Dangers.pdf.

Breidthardt, Annika (2011), 'German government wants nuclear exit by 2022 at latest', Reuters, 30 May. http://www.reuters.com/article/2011/05/31/us-germany-nuclear-idUSTRE74Q2P120110531.

Bukharin, Oleg (1997), 'Upgrading Security at Nuclear Power Plants in the Newly Independent States', *Nonproliferation Review*, Winter. http://cns.miis.edu/npr/pdfs/bukhar42.pdf

Cho, Meeyoung (2014), 'South Korea nuclear operator says cyberattacks continue, reactors safe', Reuters, 28 December. http://www.reuters.com/article/2014/12/28/us-southkorea-cybersecurity-nuclear-idUSKBN0K603320141228.

Etalle, Sandro, Gregory, Clifford, Bolzoni, Damiano, Zambon, Emmanuele and Trivellato, Daniel (2013), 'Monitoring Industrial Control Systems to Improve Operations and Security: An overview of the threats to industrial control systems and the technologies to protect them', *SecurityMatters* White Paper (San Jose, California: Cisco Systems), 1 December. http://www.secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_monitoring_EU.pdf.

Falliere, Nicolas, O'Murchu, Liam and Chien, Eric (2011), *W.32 Stuxnet Dossier*. *Version 1.4*, Symantec Security Response, February.

Ferguson, Charles and Potter, William (2005), *The Four Faces of Nuclear Terrorism* (New York: Routledge), pp. 224–25.

Fortinet (2010), 'Securing SCADA Infrastructure', White Paper (Sunnyvale, CA: Fortinet). http://www.fortinet.com/sites/default/files/whitepapers/WP_SCADA.pdf.

GAO (United States Government Accountability Office) (2008), 'TVA Needs to Address Weaknesses in Control Systems and Networks', Report to Congressional requester, May. http://www.gao.gov/new.items/d08526.pdf.

Goldman, David (2013), 'Hacker hits on U.S. power and nuclear targets spiked in 2012', *CNN Money*, 9 January. http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/.

Greenwald, Glenn (2014), *No Place to Hide: Edward Snowden, the NSA and the US Surveillance State* (London: Hamish Hamilton/Penguin Books).

Holt, Mark and Andrews, Anthony (2014), 'Nuclear Power Plant Security and Vulnerabilities', Congressional Research Service, 3 January. https://www.fas.org/sgp/crs/homesec/RL34331.pdf .

Home Office (2010), Cyber Crime Strategy, presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, March. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf.

IAEA (2014a), Department of Nuclear Safety and Security, 'Education and Training', 9 December. http://www-ns.iaea.org/training/default.asp?s=9&l=78.

IAEA (2014b), Department of Nuclear Safety and Security, 'Concepts and Terms', 9 December. http://www-ns.iaea.org/standards/concepts-terms.asp.

IAEA (2014c), Department of Nuclear Safety and Security, 'Department of Nuclear Safety and Security', 22 October. https://www.iaea.org/about/employment/ns/.

IAEA (2015), 'The Fukushima Daiichi Accident Report by the Director General and five technical volumes', http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1710-ReportByTheDG-Web.pdf.

Idaho National Laboratory (2008), 'Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program', Report prepared for the US Department of Energy, Office for Electricity Delivery and Energy Reliability, November. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/31-INL_Common_Vulnerabilities_Report.pdf.

Jonas, Val (2011), 'Five Steps to Enterprise Risk Management', Risk Decisions White Paper, January. http://riskdecisions.com/wp-content/uploads/ERM-5-steps-to-Enterprise-Risk-Management_Risk-Decisions-whitepaper_Jan11_FINAL.pdf.

Kaspersky, Eugene (2013), Talk at the Press Club in Canberra, Australia. https://www.youtube.com/watch?v=6tlUvb26DzI&feature=youtu.be.

Kesler, Brent (2011), 'The Vulnerability of Nuclear Facilities to Cyber Attack', *Strategic Insights*,10(1), Spring, pp. 15–25.

Kim, Sohee and Cho, Meeyoung (2014), 'South Korea prosecutors investigate data leak at nuclear power plants', Reuters, 21 December. http://www.reuters.com/article/2014/12/21/us-southkorea-nuclear-idUSKBN0JZ05120141221.

King, Rachel (2014), 'Security Experts Express Concern over Nuclear Cybersecurity Proposal', *Wall Street Journal*, CIO Report, 17 November. http://blogs.wsj.com/cio/2014/11/17/security-experts-express-concern-over-nuclear-cybersecurity-proposal/cv.

Krebs, Brian (2008), 'Cyber Incident Blamed for Nuclear Power Plant Shutdown', *Washington Post*, 5 June. http://www.washingtonpost.com/wpdyn/content/article/2008/06/05/AR2008060501958.html.

Langner, Ralph (2013), 'To Kill a Centrifuge' (Hamburg: Langner Group), November. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

Markey, Edward (2003), 'Correspondence between Representative Edward Markey, Senior Member of the Select Committee on Homeland Security, and Nils Diaz, Chairman of the Nuclear Regulatory Commission surrounding the Slammer worm infection at the Davis-Besse nuclear power plant, 3 November. http://pbadupws.nrc.gov/docs/ML0329/ML032970134.pdf.

Martellini, Maurizio, Shea, Thomas and Gaycken, Sandro (2012), 'Cyber Security for Nuclear Power Plants', US Department of State, 23 January. http://www.state.gov/t/isn/183589.htm.

McConnell, Bruce, Austin, Greg, Cappon, Eric and Kostyuk, Nadiya (2014), *A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets*, Policy Report (New York: EastWest Institute), January.

McCurry, Justin (2014), 'South Korean nuclear operator hacked amid cyber-attack fears', *The Guardian*, 23 December. http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack.

NTI (Nuclear Threat Initiative) (2006), 'Russian Warns of Cyber Terror Against Nuclear Sites', 9 November. http://www.nti.org/gsn/article/russian-warns-of-cyber-terror-against-nuclear-sites/.

Park, Ju-min and Cho, Meeyoung (2015), 'South Korea blames North Korea for December hack on nuclear operator', Reuters, 17 March. http://www.reuters.com/article/2015/03/17/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317.

Pederson, Perry (2014), 'A Cost-Efficient Approach to High Cyber Security Assurance in Nuclear Power Plants: The RIPE Framework as an Alternative to Regulatory Guide 5.71 and NEI 08-09' (Munich: Langner Group), April. http://www.langner.com/en/wp-content/uploads/2014/04/High-Cyber-Security-Assurance-in-NPPs.pdf.

Shin, Ickhyun (2010), 'Cyber Security on Nuclear Power Plant's Computer Systems', Transactions of the Korean Nuclear Society Autumn Meeting in Jeju, Korea, 21–22 October. http://www.kns.org/kns_files/kns/file/498%BD%C5%C0%CD%C7%F6.pdf.

Shubert, Atika (2011), 'Cyberwarfare: A different way to attack Iran's reactors', CNN.com, 8 November. http://edition.cnn.com/2011/11/08/tech/iran-stuxnet/.

Simonite, Tom (2012), 'Stuxnet tricks copied by computer criminals', *MIT Technology Review*, 19 September. http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals/.

Ten, Chee-Wooi Ten, Liu, Chen-Ching and Manimaran, Govindarasu (2008),'Vulnerability Assessment of Cybersecurity for SCADA Systems', *IEEE Transactions on Power Systems*, 23(4), November.

Tofino Security (2009), 'Case Profile: Davis-Besse Nuclear Power Plant'. https://www.tofinosecurity.com/sites/default/files/CP-103-Case_Profile-Davis_Besse-rev1.pdf.

Vincent, James (2013), 'Russian nuclear power plant infected by Stuxnet malware says cyber-security expert', *The Independent*, 12 November. http://www.independent.co.uk/life-style/gadgets-and-tech/news/russian-nuclear-power-plant-infected-by-stuxnet-malware-says-cybersecurity-expert-8935529.html.

von Hippel, Frank (2011), 'The radiological and psychological consequences of the Fukushima Daiichi accident', *Bulletin of the Atomic Scientists*, 67(5) (September/October), pp. 27–36.

Weiss, Joe (2009), 'Nuclear Plant Control System Cyber Vulnerabilities and Recommendations Toward Securing Them: Enabling Comprehensive Network-Based Security for Control Systems', Juniper Networks and Applied Control Solutions, White Paper. http://ndm.net/juniperstore/pdf/nuclear-plant-white-paper.pdf.

Zetter, Kim (2014), *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers).

The International Security Department

The International Security Department (ISD) at Chatham House produces leading research for policy-makers and opinion-shapers. The department's permanent team of specialist security experts and an extensive network of associate fellows cover a wide spectrum of issues including cyber security, nuclear security, terrorism, space security, and UK defence policy and its impact on the international arena. The ISD's research is accessible to both the public and private sectors, and seeks to develop discussion on how to tackle the threats and challenges of today. Through publications, events and international engagement, the department draws on the broad-ranging research expertise at Chatham House and the institute's international partnerships. The ISD's multidisciplinary approach to its research brings diverse perspectives and regional insights into current debates.

Recent publications include:

- *Iran and Nuclear Restraint, Lessons from Elsewhere*, Patricia Lewis (July 2015)
- *The Humanitarian Impacts of Nuclear Weapons Initiative: The 'Big Tent' in Disarmament*, Heather Williams, Patricia Lewis and Sasan Aghlani (March 2015)
- *The Arms Trade Treaty and Human Security: Cross-cutting Benefits of Accession and Implementation*, Elli Kytömäki (February 2015)
- *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, Caroline Baylon (December 2014)

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223