sipri

INTEGRATING CYBERSECURITY AND CRITICAL INFRASTRUCTURE

National, Regional and International Approaches

EDITED BY LORA SAALMAN

March 2018

Integrating Cybersecurity and Critical Infrastructure

National, Regional and International Approaches

EDITED BY LORA SAALMAN

March 2018

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: + 46 8 655 9700
Email: sipri@sipri.org
Internet: www.sipri.org

Contents

Preface

Discussions of the cyber-threats to critical infrastructure have become more frequent in the wake of the cyberattacks against Ukraine's power grid in 2015. While there seems to be a general consensus that cyberattacks resulting in damage to critical infrastructure, such as hospitals and power grids, are a common threat, there is a great deal of disagreement on how to define the parameters of and escalation within this arena. This volume reveals that much of the discussion at the national, regional and international levels continues to be disconnected and even conflicting.

From the system-level analyses of critical infrastructure to Japan's development of cybersecurity bodies, and from the creation of European Union regulations to deliberations within the United Nations, the analyses here offer the reader an opportunity to expand his or her technical, regulatory and legal understanding of cyberspace. Given the relative youth of this domain, this volume seeks to offer the reader a foundation for better understanding the current key issues and to facilitate the formation of a more common approach to integrating cybersecurity norms into critical infrastructure.

Dan Smith
Director, SIPRI
March 2018

Acknowledgements

The Stockholm International Peace Research Institute and the editor would like to express their sincere gratitude to the Government of Japan for its support of this project. The editor also wishes to thank all of the experts who contributed to this volume: Shinichi Yokohama, Head, Cybersecurity Integration, NTT Corporation (Japan); Dr Peter Bernard Ladkin, Professor, Computer Networks and Distributed Systems, University of Bielefeld, Germany (United Kingdom); Colonel (retd) Gary Brown, first Senior Legal Counsel, US Cyber Command (United States); Dr Keiko Kono, Senior Fellow, National Institute for Defence Studies, Japan Ministry of Defense (Japan); Dr Eneken Tikk, Head, Strategy and Power Studies, Cyber Policy Institute, Finland (Estonia); and Sarah Backman, Consultant, Secana Cybersecurity (Sweden), as well as the other workshop speakers, Junjiro Isomura, Senior Fellow, Director, US-Japan Strategic Summit Program, Hudson Institute, United States (Japan); Dr Page Stoutland, Vice President, Scientific and Technical Affairs, Nuclear Threat Initiative (United States); John Strand, Founder, Black Hills Information Security (United States); Éireann Leverett, Founder, Concinnity Risks (United Kingdom); Dr Motohiro Tsuchiya, Professor, Keio University (Japan); and Erik Zouave, Researcher, Swedish Defence Research Agency (FOI) and Centre for Information Technology and Intellectual Property Law, KU Leuven, Belgium (Sweden).

Abbreviations

CCFD	Causal Control Flow Diagram
CERT-EU	Computer Emergency Response Team of the European Union
CISO	Chief Information Security Officer
CSF	Cross-Sector Forum
CSHQ	Cybersecurity Strategy Headquarters (Japan)
CSIRTs	Computer Security Incident Response Teams
DDoS	Distributed denial of service
DLNN	Deep-learning neural-network
EAM	Emergency action message
EC3	European Cybercrime Centre
ENISA	European Union Agency for Network and Information Security
FS-ISAC	Financial Services Information Sharing and Analysis Centre
GDPR	General Data Protection Regulation
IACS	Industrial Automation and Control Systems
ICBM	Intercontinental ballistic missile
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IHL	International Humanitarian Law
IPA	Information Technology Promotion Agency
ISAC	Information Sharing and Analysis Centre
IT	Information technology
IT-ISAC	Information Technology-Information Sharing and Analysis Centre
JSDF	Japanese Self-Defense Forces
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NCA	Nippon CSIRT Association NCA
NCIRC	NATO Computer Incident Response Capability
NICT	National Institute of Information and Communications Technology
NIS	Network and information security
NISC	National Information Security Centre
NTT	Nippon Telegraph and Telephone Corporation
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Executive summary

On 18 December 2017, SIPRI held a workshop, 'Japan–Europe–USA: Integrating Cybersecurity and Norms into Critical Infrastructure'. The key findings of the workshop are set out below.

Overall

1. Many engineered systems that depend on digital-computational parts can be 'hacked'. The financial systems sector and militaries have been dealing with such threats for many decades and the development of protection and countermeasures is often known as information-systems security or information technology (IT) security. Within this discourse, integrity is part of the 'CIA triad', which consists of the key IT-security system properties of confidentiality, integrity and availability.
2. Reliability and availability are well-defined pure system properties, but accountability and confidentiality also involve people. Critical infrastructure comprises many systems, such as the power supply and the power grid, the water supply, wastewater treatment and transportation, which have come to make extensive use of digital computers. Some of these digital-computational systems are not primarily information systems, but also engage in behaviour that means having to factor socio-technical control systems into how system integrity is defined and protected.
3. Extensive security gaps at all levels of society are continuously exploited for a variety of purposes, such as financial gain, political influence, hacktivism, espionage, industrial espionage and even cyberwarfare. Examples include: the distributed denial of service (DDoS) attacks on Estonian Government websites in 2007; the Zeus 2009 banking Trojan, which stole banking information; the Stuxnet worm in 2010, which attacked Iranian nuclear centrifuges; the cyberattacks on a German steel mill in 2014; the attacks on Ukraine's power grid in 2015; and the Wannacry ransomware attacks on hospitals in 2017.

National

1. The Japanese Government identifies 13 critical infrastructure sectors: information and communications, finance, aviation, railways, electricity generation and supply, gas, government and administrative services, medical services, water supply, logistics, chemicals, credit card infrastructure and petroleum. The National Information Security Centre (NISC) is tasked with promoting close cooperation among various actors, from critical infrastructure

operators to ministries, in the fields of financial services, internal affairs, health and welfare, and economic policy, as well as transport and infrastructure.

2. Japan's Cybersecurity Strategy Headquarters is considered the 'control tower' for the cybersecurity field. Within this structure, the NISC has been assigned various tasks, such as performing continuous network monitoring, conducting cybersecurity audits and engaging in analyses of serious incidents. Its responsibilities are limited in scope, however, and cover only central government bodies, incorporated administrative agencies and designated corporations. As a result, the NISC is not able to respond to incidents or cyberattacks that do not fall within its jurisdiction.
3. The Japanese Government distinguishes between two discrete types of large-scale cyberattack: cyber-enabled armed attacks and cyberterrorism. To address these threats, in 2014 the Japan Ministry of Defense (MOD) established a Cyber Defence Group under the Command, Control, Communications and Computer Systems Command. However, the Cyber Defence Group only responds to cyber-threats carried out against the Japanese Self-Defense Forces' (JSDF) own network.
4. If the JSDF were to assume new cyber-missions in the future, according to pre-existing domestic law, its operations should not involve the use of force. The Tallinn Manual 2.0 argues that a target state is prohibited from using force when it takes countermeasures or acts pursuant to the plea of necessity in response to serious cyberattacks. That said, the concept of a 'use of force' in cyberspace is unclear, as is the meaning of 'offensive'.
5. The Japanese Government has been undertaking a variety of essential initiatives to ensure security in cyberspace. The Basic Law on Cybersecurity passed the Japanese Diet in November 2014, and Japan's Cybersecurity Strategy was approved in 2015. The Fourth Action Plan for Critical Infrastructure Protection was launched in April 2017. These government efforts are the foundations for ensuring Japan's cybersecurity. Advances at the governmental level notwithstanding, 90 per cent of Japan's information and communications technology (ICT) assets are owned by the private sector.
6. The Japan Business Federation (*Keidanren*), which is the largest business federation of sectoral trade associations, announced its cybersecurity principles in 2017. These principles clearly state that 'self-help' by individual companies serves as the starting point for cybersecurity. Only after individual companies have engaged in efforts to improve their own standards and conditions can effective collaboration take place. Having passed the litmus test of engaging

in self-help and collaborative improvements, these firms are then eligible for support from the government.

7. The number of Japanese firms that have established Computer Security Incident Response Teams (CSIRTs) is expanding. The Nippon CSIRT Association (NCA) is a non-profit organization that helps companies build up such teams. On joining, companies are offered support with building and strengthening their CSIRTs from other NCA members with more developed practices. At the sectoral level, Information Sharing and Analysis Centres (ISACs) have been formed across Japan. A group of more than 40 companies from various sectors formed the Cross-Sector Forum (CSF) in 2015 to collaborate on capacity building and information sharing.

Regional

1. The development of European cybersecurity measures has been swift, particularly since the publication of the first European Union (EU) cybersecurity strategy in 2013. The strategy identifies three main 'pillars' of cybersecurity: societal security or network and information security (NIS), cybercrime prevention and cyber-defence. While interconnected and overlapping, each pillar has specific features. The European Cybercrime Centre (EC3) plays a major role in cybercrime prevention, engaging in activities such as operational coordination among member states, awareness initiatives, early warning notifications, threat assessments and decision-making support regarding cybercrime prevention and management.
2. The two dominant malware threats encountered by EU law enforcement are ransomware and information theft via malware. Social engineering is a common component of these attacks, since the human component is often the weakest link in the chain. Attacks targeting individuals are common in the cybercrime pillar, and can include identity theft, sexual exploitation, payment fraud and stolen personal information. An important measure within this pillar is the EU General Data Protection Regulation (GDPR), which enters into force in May 2018 and seeks to strengthen the rights to privacy of individuals and the management of personal information.
3. The European Union Agency for Network and Information Security (ENISA) is an important actor in the societal security or NIS pillar. It conducts pan-European cyber-crisis exercises, enhances cybersecurity awareness, supports member states as they build capacity and promotes collaboration and information sharing. The cyber-defence pillar is the least developed, since EU involvement in this area remains a sensitive issue. However, several initiatives have been introduced to enhance collaborative capacities and exchange instruments between the EU and the North Atlantic

Treaty Organization (NATO), such as the Technical Arrangement on Cyber Defence, which was concluded between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU) to exchange information and share best practices among emergency response teams.

International

1. International norms typically develop through years of state practice in a given area. Through repeated trial and error, states reach accommodations with each other and eventually determine the best approach to avoiding conflict. Over time, these practices can develop into international law. Unlike national activities in more traditional areas of international relations, state practice in cyberspace is generally not disclosed. While there might be speculation about the perpetrator of a cyber-incident, unless states publicly take responsibility for an action or event, there is no foundation for developing patterns of state practice that inhibit the development of international norms.
2. At the heart of a norm lies informal agreements among states and practices that have accumulated over time. While negotiations may then lead to formal and enforceable international agreements, norms are informal and unenforceable standards of behaviour. Efforts to craft some standards continue—and the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) provides some reasons for optimism. Nonetheless, in 2017 the UN GGE failed even to agree that International Humanitarian Law (IHL) applies in cyberspace. The process failed partly because states continue to avoid placing their cyber-strengths on the table for negotiation.
3. When seeking means to develop cyber-norms, one of the best initial steps is to concentrate international efforts on repeated state practice and work towards bilateral agreements between allies. If a number of states partner with even one other state to agree on certain norms of behaviour, common elements from several bilateral agreements can serve as a starting point for the development of international norms. Despite the challenges, international norms may well offer the best path to stability and the protection of critical infrastructure.
4. In spite of the tendency to view the 2017 lack of consensus at the end of the UN GGE meeting as a failure, there are areas of progress on which the process can build. While recognizing fundamental differences among states about several principal issues, such as the legally binding nature of due diligence, the emphasis on national versus international efforts and the nature of the threat, experts

have managed to find common ground and surprising coherence in their recommendations. They have also provided a checklist for states that are seeking to counter cross-border threats to their critical infrastructure.

Conclusions

1. While progress has been made in terms of Japan's establishment of organizations to monitor and respond to cyberattacks, ongoing questions of jurisdiction at the national level hinder the ability to coordinate both preparation and response. Long-standing policies constraining the role of the JSDF have led to questions about the role it could play outside of its narrowly defined parameters in the event of a large-scale cyberattack on Japan's critical infrastructure. Groups such as the NISC also remain limited in terms of their response, in that their domestic jurisdiction could leave gaps.
2. The EU poses a unique challenge in that it is a highly integrated body of countries that are still struggling to integrate both their regulatory frameworks and their information sharing practices in cyberspace. This places in high-relief the difficulty of coordination among even like-minded countries on defining and responding to cyber-incidents. Moreover, expanded regulatory priorities on information security combined with efforts to enhance information sharing may encounter future tensions. A preponderance of regulation and checklists does not necessarily lead to greater protection of critical infrastructure, particularly if basic cyber-hygiene remains weak.
3. Navigating the diverse stances among nations will be essential in order to reach comity on the risks of cyberattacks to critical infrastructure. Nonetheless, the lack of a consensus at the UN GGE in 2017 demonstrates that countries remain divided on even the most basic tenets of IHL and the nature of information security and cybersecurity. To remedy this, greater efforts among like-minded states at the bilateral and 'mini-lateral' levels could serve as a foundation for building up a series of norms that can be incrementally integrated into the international level. Such coalition building, however, could also lead to greater fragmentation by region or technical capacity.
4. The integration of norms at the international level is likely to depend on the establishment of such norms at the national and regional levels. Unfortunately, as in any number of arenas, the domain of cyberspace may have to suffer a large-scale attack on critical infrastructure before an actionable impetus can be found for systemic, industrial and legal change at the national, regional and international levels.

1. Introduction

SIPRI held the workshop 'Japan–Europe–USA: Integrating Cybersecurity and Norms into Critical Infrastructure' on 18 December 2017. The event assembled 12 leading academic, political, military, technical and legal cybersecurity experts from Japan, Sweden, the United Kingdom, Estonia and the United States, as well as an audience of over 30 ambassadors, defence attachés, senior scientists and industry experts, to discuss definitions and threats to critical infrastructure, case studies on cyber-intrusions and attacks, and concrete ways forward on national, regional and international cooperation. Dr Lora Saalman, Associate Senior Fellow at SIPRI and Vice President of the Asia–Pacific Program at the EastWest Institute, moderated the workshop. This volume seeks to delve deeper into a few of the target areas of cybersecurity and critical infrastructure highlighted at the workshop, such as system integrity, the role of the private sector and legal frameworks. Contributing authors discuss these domains at the national, regional and international levels.

In chapter 2, Dr Bernard Ladkin analyses the impact of cyberattacks on critical infrastructure at the most basic level—the system level. In discussing system integrity, he provides a framework for better understanding how to evaluate the functioning of a system when external inputs affect its original state and environment. He applies this scientific analysis to the case of US command and control as it pertains to its intercontinental ballistic missile launch capabilities. While he concludes that greater information is needed to determine the vulnerability of such systems to cyberattack, he argues that the human component in these processes and systems allows for greater susceptibility to disruption. Dr Keiko Kono expands this discussion of the potential for disruption to the national level, probing the question of whether the Japanese Government should consider changing its defence policy and assigning new missions to the Japanese Self-Defense Forces (JSDF) in the cyber-domain. She emphasizes that the National Information Security Centre (NISC) is not able to respond to incidents of cyberattacks that do not fall within its jurisdiction, constraining the country's ability to respond to a cyberattack on the integrity of its critical infrastructure. She posits that the JSDF could play a larger role in coordinating Japan's preparations for and response to such attacks. She emphasizes that the role of the international community in creating norms against the use of cyberattacks against critical infrastructure is integral to Japan formulating its longer-term national strategy.

In chapter 3, Shinichi Yokohama offers an overview of the arena in which most information and communications technology (ICT) assets continue to reside—the private sector. He argues that while Japan has increasingly built up its cybersecurity practices through the establishment by various companies of Computer Security Incident Response Teams (CSIRTs), as coordinated by the Nippon CSIRT Association (NCA), the level of integration of standards and information sharing must also be expanded. Citing the 2020 Olympics and Paralympics to be held in Tokyo, Yokohama notes that these will not only be a test of the durability of

Japan's cybersecurity and critical infrastructure integration, but also a foundation that will hopefully lead to long-term, sustainable improvements to the existing nascent framework. Broadening the aperture, Sarah Backman explores how Europe is working to integrate cybersecurity regulatory bodies and standards at the regional level. Citing the EU General Data Protection Regulation (GDPR), which enters into force in May 2018, she notes the importance of information security as part of the construct of critical infrastructure. To this end, she cites the European Union Agency for Network and Information Security (ENISA) as an important actor due to its pan-European cyber-crisis exercises. Nonetheless, she notes that information sharing remains a significant hurdle when it comes to EU member states communicating sensitive cybersecurity findings.

In chapter 4, Colonel (retd) Gary Brown provides insights into the difficulty of integrating a common legal framework and norms into cyberspace and critical infrastructure at the international level. He cites the absence of public practice as an impediment to negotiating norms, since the premise of customary law on which informal state agreements and practice have accumulated over time does not exist in the cyber-domain. In particular, the difficulty of attribution coupled with the unwillingness of states to reveal their participation in or the origins of cyberattacks make it difficult to establish a history of state behaviour or precedence upon which to base this foundation. While Brown finds some reason for optimism in the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) process, he observes that its failure in 2017 to reach a consensus even on standards rooted in International Humanitarian Law does not bode well. Instead, he suggests that the most viable means of integrating a foundation for future norms will be to concentrate on repeated state practice and work towards bilateral agreements between allies, providing the foundation for future international norms. Dr Enekin Tikk reviews the no-consensus outcome of the fifth round of the UN GGE in 2017. While she notes that this outcome derives in part from fundamental differences among states on such issues as the legally binding nature of due diligence, emphasis on national versus international level efforts and the nature of the threat, the UN GGE process still offers a degree of progress and common ground. She argues that although several countries regard the protection of critical infrastructure primarily as a national responsibility, most seem to agree that as a minimum, exchanges of best practices and national experience are necessary to provide effective guarantees against critical infrastructure-related cyberattacks. As a result, she contends that this common assessment can provide a foundation on which to build future norms.

2. System integrity and the national level

2.1. Dissecting system integrity and missile launch

PETER BERNARD LADKIN[1]

Introduction

It is common knowledge that many engineered systems that depend on digital-computational parts can be 'hacked'. This means that intruders, people or software that are not part of the normal system functioning can gain access to the system functions and subvert them. The financial systems sector and militaries have been dealing with such threats for many decades now, and the development of protection and countermeasures is known as information technology security or IT security.

Within this discourse, integrity is one of the 'CIA triad', which consists of the key IT-security system properties of confidentiality, integrity and availability. Additional essential elements, such as authenticity, accountability, non-repudiation and reliability, are considered in International Electrotechnical Commission (IEC) documentation.[2] This is quite a heterogeneous grouping. For example, reliability and availability are well-defined pure system properties, but accountability and confidentiality also involve people.

Critical infrastructure includes an array of systems, such as power supplies and grid, water supply, wastewater treatment and transport networks, which all make extensive use of digital computers. Some of these digital-computational systems are not primarily information systems, but also engage in behaviour. In other words, they control processes such as the generation of electricity from a turbine, ensuring that system security is preserved and that the intended behaviour of such systems is not subverted. Such systems are called industrial automation and control systems (IACS). The term 'cybersecurity' covers IT security as well as the security of IACS. This section focuses on the integrity of control systems, with particular attention paid to an example based on a socio-technical control system—missile launch.

Integrity as a concept

What is system integrity and why is it important? When discussing the integrity of persons, this means that a person does not subvert social and business transactions, by keeping promises and meeting obligations, as well as demonstrating financial and contractual honesty. System integrity is similar, but the definition

[1] Dr Peter Bernard Ladkin is a Professor of Computer Networks and Distributed Systems at the University of Bielefeld in Germany. The author gratefully acknowledges the support of the German Federal Ministry for Economic Affairs and Energy (BMWi) (Grants: 03TNG006A and 03TNG006B).

[2] International Electrotechnical Commission, IEC 27000: 2016, Information technology, Security techniques, Information security management systems, 'Overview and vocabulary', IEC, 2016.

is far from clear. For example, the IEC defines the international standard for security of IACS as the 'quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data'.[3]

This description is further explained by a note that states, 'in a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information'.[4] This clarification hews closely to the International Federation for Information Processing definition of integrity as 'absence of improper system alterations'.[5] This creates a conundrum in determining which definition applies: logical correctness, completeness and consistency or no unauthorized/improper modification. Which is the essential function of the system? To answer this query, the international standard for functional safety of IACS defines 'safety integrity' as the 'probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time'.[6]

So, rather than adhering to the concept of a person with integrity 'doing the right thing', these systems operate within a probabilistic spectrum. To scientists and engineers, a probability is a real number between 0 and 1. This indicates that this definition has very little to do with logical correctness and completeness, much less no unauthorized/improper modification. If this formulation seems confusing, it is. The field of experts should be able to present a more comprehensible definition of the concept of integrity of systems and this essay attempts to do so with a real-world example.

System quirks

Human-designed systems are deliberately causal objects. System components are designed to have specific effects on the environment in which the system operates, on other system components and parts, or on both. An entity that engages in behaviour can be labelled as an 'agent'. A 'system' is simply a collection of agents that engage in behaviour. A system has a 'boundary', which is the distinction between entities that belong to the system and those which do not; and it has an 'environment', which is those entities that do not belong to the system but interact with it. In other words, these entities engage in relations with system agents and have causal power to modify these relations over time. Some systems occur

[3] Definition 2.1.55 of International Electrotechnical Commission, IEC TS 62443-1-1:2009, Industrial communication networks, Network and system security, Part 1-1, 'Terminology, concepts and models', IEC, 2009.

[4] Definition 2.1.55 of International Electrotechnical Commission, IEC TS 62443-1-1:2009 (note 3).

[5] Laprie, J. (ed.), *Dependability: Basic Concepts and Terminology*, vol. 5, *Dependable Computing and Fault Tolerance* (Springer-Verlag: Vienna, 1992); Avizienis, A. et al., 'Basic concepts and taxonomy of dependable and secure computing', *IEEE Transactions On Dependable and Secure Computing*, vol. 1, no. 1 (Jan.–Mar. 2004), pp. 1–23.

[6] Definition 3.5.4 in International Electrotechnical Commission, IEC 61508-3, Functional safety of electrical / electronic / programmable electronic safety-related systems—Part 4—Definitions and abbreviations, 2nd edn, 2010.

naturally and some are deliberately engineered by people. This analysis focuses exclusively on engineered systems.

Systems sometimes perform the task assigned to them and at other times they do not. This means that they sometimes fail to do anything even when a human agent has tasked them to do something. They may be purely physical as in the case of a bicycle, but may also include human agents as in the case of an air-traffic control system. In the latter case, these are 'sociotechnical' systems. A scheduled railway train is a sociotechnical system, with a physically engineered train on a physical track, a remote human controller and a driver responding to physical-train dynamics, signals and other events. A signalling system has many more purely physical components today than it did when people in signal boxes moved mechanical components to activate semaphore signals. An important part of a modern signalling system and its operation is the display of information to a train controller, his or her processing of that information and the decisions and signalling actions that result. Information, defined by its veridicality and its flow, is an important component of many sociotechnical systems, such as train operation. Train operation itself is part of a more complex sociotechnical system: railway operation.

Engineered systems are usually teleological, that is, they were designed by people with a specific function or a specific goal in mind—the functional requirements. Most effective systems are accompanied by documentation that provides formal articulation of the 'functional requirements specification'. Once the requirements have been determined, the next phase is the design of the object such that it achieves the desired effect, followed by implementation. The system works if implementation fulfils the system design specification, and the design specification in turn fulfils the requirements. Although this might all seem simple, those who are not system engineers might be surprised by how inadequately these crucial steps in system-building are often performed.

Distinguishing functional behaviour from other behaviour is crucial, since agents will typically engage in behaviour that is not part of the system function. As one visceral example, circuit boards that have been bathed in acid would engage in different behaviour, which may not be part of their specified function. As such, the environmental conditions of the system will ensure to the greatest extent possible that such boards will not be bathed in acid while executing their system function. Air traffic controllers enter even more variables into this matrix, as they eat, sleep, watch movies and engage in other behaviour irrelevant to the casual operation of air traffic control systems.

Given this basic set of parameters, systems may malfunction through inadvertent or deliberate causes in many different ways. A crude taxonomy is set out below:

1. A system may encounter an environmental situation for which it has not been conceived or designed and behave in an inappropriate way. This may be labelled a 'requirements error'. In other words, the system requirements did not cover all situations to be encountered. For example, the working environment of a system may occasionally

exceed the temperature range within which its digital electronics reliably function.

2. A system may have a flaw in its design or implementation so that it reacts in an inappropriate way to an environmental situation foreseen in the requirements. This is a 'design error' or 'implementation error'. In software, these are often called bugs.
3. Specific agents in a system may malfunction. In other words, in circumstances in which they previously behaved appropriately, they no longer do so. A circuit board may burn out or an operator may fail to register and then to act on crucial information. A human-agent malfunction is often said to be a 'human error'.
4. Components require maintenance, which constitutes physical attention over time to ensure they continue to play their intended functional role. Agents must often be interchangeable, such that circuit boards can be swapped out for newer boards and human operators can go off-shift to be replaced by other operators. We can call the processing of such phenomena 'functional maintenance'. During this maintenance, it may be that certain system components lose or change part of their functional behaviour or, in other words, that the agent loses functional integrity.
5. Changes may occur to systems other than through functional maintenance. Some humans may deliberately try to compromise functional integrity by introducing components, or changes to components, with a different functional behaviour than expected or specified. Such components or portions of components are often called malware. These may be hardware or software, or both. When malware is introduced into a system component, that component loses functional integrity.

Given these examples indicating scenarios in which functional integrity is lost, we define functional integrity as 'the property of a system or component such that its system-relevant behaviour remains the same'. In clarifying this definition, system-relevant behaviour denotes the behaviour of a system or a component of a system that contributes causally to the fulfilment of some part of the 'system requirements specification'. Malware in a purely software-driven system may cause it to behave in ways non-conformant with its specification or the expectations of its stakeholders. However, malware in a sociotechnical system does not always affect system functionality in quite the same way.

For example, a physical system may have as its partial function to provide information to a human agent, who then acts on that information. This would equate with an air-traffic controller looking at a radar display of current aircraft positions and movements, and adjusting them through verbal instructions to pilots. It could also be applied to an operator in a nuclear power plant checking that all the gauges are showing normal readings and acting on any abnormality.

Malware may corrupt the information displayed, so that the picture of the world or partial world-state differs from reality. This may happen even though the system retains functional integrity as defined above. This situation occurs in sociotechnical systems that do not display malware influence.[7] A human agent, an operator, may treat non-veridical information as correct and act accordingly. In doing so, he or she would propagate behaviour appropriate to the falsified situation through the system. Alternatively, the operator may notice an anomaly and take action to validate the information or otherwise mitigate its effect on system behaviour, thereby smoothing the effect of the anomaly.

Human agents are traditionally used in critical system operations to play such an anomaly-smoothing role. As is well known, however, they can also indulge in inappropriate action *sui generis*, even on veridical information. For a variety of reasons, these activities would fall into the category of human error. Analysis of the conditions under which a veridical or anomalous causal chain of information is passed through a human operator could be called 'semantic safety'.[8] Analysing semantic safety requires an explicit meaning to be assigned to information displayed to an operator. *Meaning (D)* would be defined by the physical aspects of the *display D*. This allows the question to be asked whether, and if so how, the operator uses *Meaning (D)* in his or her further deliberations and actions within system operation.

In a situation in which *Meaning (D)* is non-veridical and the *operator O* induces actions which are inappropriate, the functional integrity of the system causally downstream from *O* may remain intact. However, because of the actions taken on misleading critical information in *Meaning (D)*, the computation causally downstream of *O* has been corrupted. This situation can also be categorized as a loss of integrity, but it is not due to a lack of functional integrity causally downstream of *O*. The situation causally downstream from *O* has been generated by the non-veridical information in *Meaning (D)*.

Thus, it is crucial to delineate information integrity in the following manner: A system generally includes two types of information. First, information that reflects real-world parameters. This information might be veridical (it has the same value as the real-world parameter) or non-veridical (it has a different value from that pertaining in the real world). Second, information internal to the system that has limited or no correspondence with parameters outside the system.

This leads to separate clauses in the definition of 'information integrity'. In the first clause, information integrity is the property that the meaning of the information held at any state *St* of the system *Sys* is conformant with either: (*a*) the real world, such that the information corresponding to real-world parameters is veridical; or (*b*) veridical information held at other states *St1* of the system, transformed by the functionally correct transformations applied by *Sys* to *St1*, resulting in the

[7] Ladkin, P. B., 'Verbal communication protocols in safety-critical system operations', eds D. Gibbon and A. Mehler, *Handbook of Technical Communication* (Mouton de Gruyter: Berlin, 2012).

[8] Ladkin, P. D., Message to the System Safety Mailing List, 25 Aug. 2016; and Ladkin, P. B., 'OHA of a pressure tank: Digital system safety, mostly qualitative aspects', Unpublished e-textbook, Bielefeld University, 2017, <https://rvs-bi.de/publications/RVS-Bk-17-02.html>.

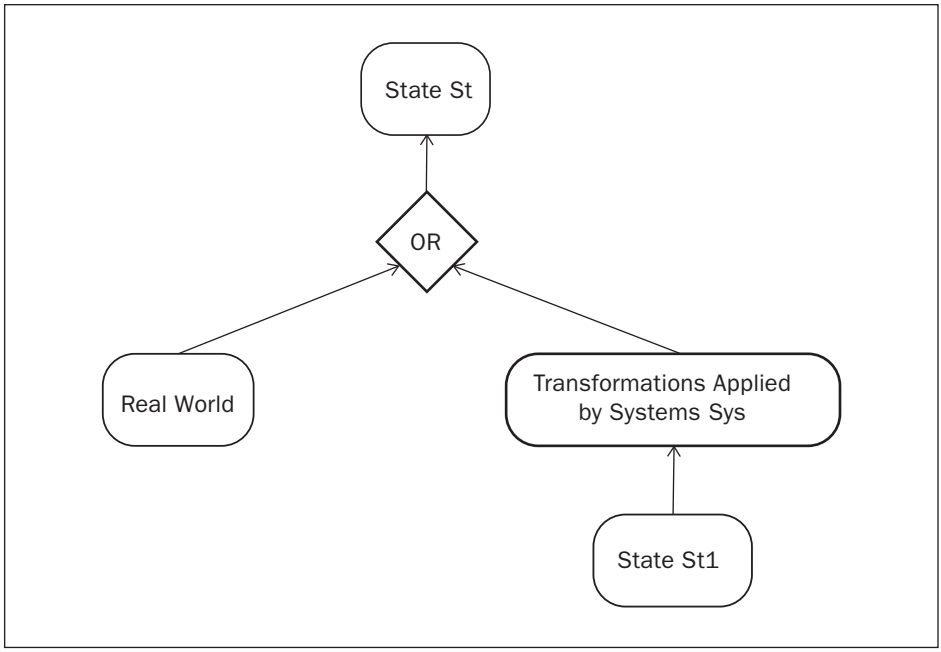

Figure 2.1.1. CCFD illustrating the definition of information integrity

St = state, Sys = system.

Source: Author compilation designed by Tim Schürmann using SERAS® YBT4 Beta.

state *St*. The situation is illustrated in the Causal Control Flow Diagram (CCFD) in figure 2.1.1.[9]

Critical example

The launching of a US intercontinental ballistic missile (ICBM), or a series of ICBMs, is a complex process of a complex system. The system involved in a launch from decision to execution is highly distributed and highly dependent on its communications infrastructure. System dependability requirements are near-absolute and the sociotechnical-algorithmic complexity to assure dependability is daunting. As befits a technology that is critical to the future of humankind, the reliability and integrity issues of the launch process have been discussed extensively in unclassified literature.[10] To this end, it is helpful for cybersecurity

[9] A CCFD is a mathematical discrete directed graph with nodes (boxes) and arrows. The arrows indicate causal relations between the nodes. The node at the tail of an arrow is a necessary causal factor of the node at the head (with the exception of 'or' nodes, which are purely formal, and which play an intuitively obvious semantic role, in that one or other of the factors at the tail is a necessary causal factor of the node after the 'or' node).

[10] Blair, B. G., *Strategic Command and Control: Redefining the Nuclear Threat* (Brookings Institution Press: Washington, DC, 1984); Ellsberg, D., *The Doomsday Machine: Confessions of a Nuclear War Planner* (Bloomsbury Publishing: London, 2017); Blair, B. G., 'Why our nuclear weapons can be hacked', *New York Times*, 14 Mar. 2017; Mackenzie, D., *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (MIT Press: Cambridge, MA, 1990); Sagan, S. D., *The Limits of Safety* (Princeton University Press:

analysis to dissect the process into components and their causal relations, in order to better consider the integrity of each.

A launch decision by the US President is communicated to the physical command centres by an Emergency Action Message (EAM).[11] An EAM is a command sent by the US President to commence system action, including launch, and is roughly comparable in length to a tweet.[12] An EAM is encrypted and cryptographically authenticated. It is a system requirement that a valid launch EAM results inevitably in a launch. This chain of activities is described in the CCFD in figure 2.1.2.[13] CCFDs were developed for use in engineered systems and can also be used to analyse sociotechnical systems such as an ICBM launch system with a semantic adaptation.

It is a complex philosophical problem to speak of 'cause' when considering human agency, since such causal agency does not necessary satisfy the counterfactual test, which is the causal criterion used in CCFDs.[14] It suffices here to identify a sociological cause of an executed action with a human or organizational intention to execute the action as defined or implied by standard system procedures. If the action is not executed, it cannot have a cause. For this example, a CCFD with this sociotechnical adaption will be referred to as a 'quasi-CCFD'. A quasi-CCFD differentiates human from physical causal agency through its notation.

Launch function

A general quasi-CCFD of the launch process is shown in figure 2.1.2. The lower nodes, which 'causally' feed into the launch decision, do not necessarily satisfy the counterfactual test. As the deciding factor, the US President is not bound by procedure to take these elements into account.[15] Various phenomena such as 'phenomenology' and 'checklist and procedures' are causally or quasi-causally input into the 'Launch Decision and Action', which then causally results in EAM commands launch via intermediate causal apparatus, denoted in the CCFD as *Syst2*.

Princeton, NJ, 1993); Schlosser, E., *Command and Control* (Penguin Books: London, 2013); and Shatz, A., 'The president and the bomb', *London Review of Books*, 16 Nov. 2017, pp. 3–6.

[11] Schaum, E. and Marcel, H., 'EAMs and HF-GCS', Numbers Station Research and Information Center, 1 June 2016.

[12] A tweet is a message sent on the internet broadcast-messaging service Twitter and was at the time of writing up to 140 alphabetical characters in length.

[13] Sieker, B., *Examples of Reverse Engineering* (Causalis Limited: London, 2012); and Ladkin, P. B., *Causal System Analysis* (Springer: London, 2006), pp. 115–36. In this volume, they were called 'Causal Influence Diagrams' (CID), which was later discovered to be an overused term.

[14] A technical test, the counterfactual test (CT), based on Lewis D., 'Causation', *Journal of Philosophy*, vol. 70, no. 17 (Oct. 1973), pp. 556–67, establishes whether a node is a necessary causal factor of another. Lewis D., *Counterfactuals* (Wiley-Blackwell: New Jersey, 1973); and RVS Group, the Why-Because Analysis Home Page, [n.d.], <https://rvs-bi.de/research/WBA>. The CT for 'A is a necessary causal factor of B' is: had A not happened, all other things being equal, would B have happened? If the answer is no, the CT is fulfilled. If the answer is yes or maybe, then the CT is not, or not necessarily, fulfilled.

[15] There has also been some public doubt expressed by experts that the US President is the sole decider. See Ellsberg (note 10); Evidence from a former US administration is available at 'Documents on Predelegation of Authority for Nuclear Weapons Use', National Security Archives, George Washington University, Washington, DC, <https://nsarchive2.gwu.edu//news/predelegation/predel.htm>.

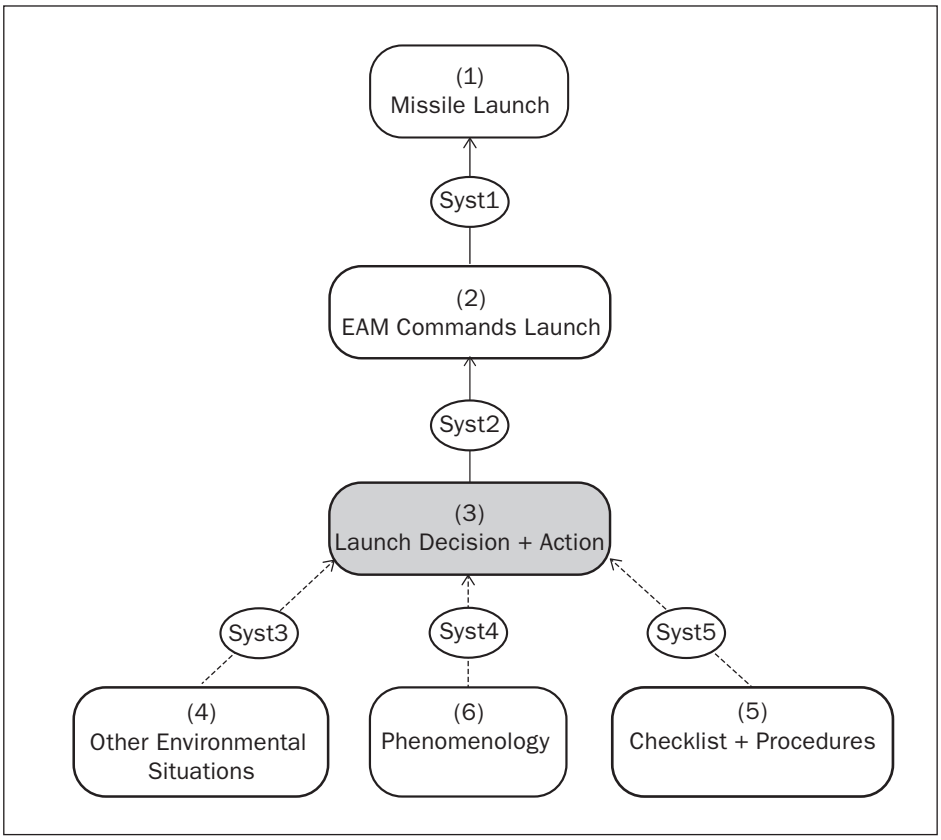

Figure 2.1.2. Quasi-CCFD of the (nominal) launch process

EAM = emergency action message; Syst = system.

Source: Author compilation designed by Tim Schürmann using SERAS® YBT4 Beta.

The EAM issued causally results in 'Missile Launch' via intermediate causal apparatus denoted *Syst1*.

A 'dual phenomenology' is used to aid launch decisions. This phenomenology consists of real-time information about possible missile launches by adversaries and comprises infrared data from satellites and dynamic data from multiple radar sites. These two data streams are generally assumed to be independent. The dual phenomenology is intended to consist of two important causal inputs, which should cohere in any launch decision. Other important causal inputs are: (*a*) the applicable checklist; (*b*) the applicable procedures; and (*c*) possibly other environmental parameters, such as information communicated by military aircraft in flight.

The above-mentioned elements are intended to form causal factors for decisions on activation of the system. The information is causally intermediated on its way to the launch decision by systems designated in figure 2.1.2 as *Syst3*, *Syst4* and *Syst5*. System designers stipulate that there is causal influence from these inputs

on the decision but, as noted above, it is possible that the influence is absent.[16] The arrows are thus not causal per se. Instead, they are 'desired-to-be-causal', since there is no mechanism to ensure that these factors are indeed causal. As a result, they do not satisfy the counterfactual test. To illustrate this distinction, figure 2.1.2 uses dashed lines to distinguish them from those nodes whose causal relations are established through the counterfactual test.

It may well be that the dashed arrows between *(6) Phenomenology* and *Syst4* are in fact causal rather than just desired-to-be-causal. This could also be applied to the arrows between *(4) Other Environmental Situations* and *Syst3*, as well as *(5) Checklist and Procedures* and *Syst5*. More detailed inquiry into the nature of these subsystems and causal connections may either strengthen or counter this assertion.

Between each of the major labelled nodes are *Syst1* … *Syst5*, which each represent a causally intermediary system apparatus. To illustrate, let us consider *Syst1*, the causal system intermediating between the production of an EAM commanding a launch and the actual launch of a missile. When a launch-EAM is produced: (*a*) communications systems transmit this EAM to the site of the missile to be launched; (*b*) at the launch site, the authenticity of the message is validated by a sociotechnical subsystem; and (*c*) if the authentication validates, action to launch the missile is then taken by that sociotechnical subsystem.

These are three separate system functions which serially combine to connect causally the production of an EAM commanding a missile launch with an actual missile launch. This subsystem *Syst1* is thus a combination of geographically separated communications and the on-site sociotechnical subsystem. Rather than this flat delineation, one might split *Syst1* into two subsystems, the second of which itself disaggregates serially into two components: (*a*) the communications subsystem *Syst1.1* conveys the US President's launch decision encoded in an EAM to the launch site, and (*b*) the on-site sociotechnical subsystem *Syst1.2* validates the EAM and acts to launch. *Syst1.2* itself splits into the serially executed subsystems: (*a*) on-launch-site reception, decoding and validation of the authenticity of the EAM; (*b*) if a launch-EAM validates, action to launch the missile.

Such a disaggregation helps to localize the various vulnerabilities which may be manifest through the impact of emerging technologies:

1. It has been suggested that the on-site sociotechnical subsystem *Syst1.2* is fairly robust against cybersecurity threats posed by emerging technologies.[17] This is largely because the procedures are human and static, and validation is largely physical rather than digital-electronic.

[16] Shatz (note 10).

[17] The referenced workshop was conducted under the Chatham House Rule. Chatham House and the Stanley Foundation, 'Mapping the Relative Risks Emerging Technologies Pose to Nuclear Weapons Systems', Workshop at Chatham House, 18–19 July 2017.

2. On general grounds, system scientists may well be concerned about the cybersecurity of the communications subsystem *Syst1.1* and the possible means of inhibiting or 'spoofing' an EAM.[18]

The caveat 'fairly robust' is apt for the cybersecurity of *Syst1.2*. It is not possible to reasonably speak of security in absolute terms—although it is possible to do so for insecurity.[19] In addition, a *Syst1.2* common cause electronic fault has indeed occurred on-site, as noted by Bruce Blair, a former ICBM launch control officer.[20] In this incident, a fault was present, but a failure was only potential. The fault would have inhibited a launch on a launch-EAM, had such an EAM been issued. Since no such EAM was issued, the fault did not manifest as failure behaviour.

Applying the terminology of integrity to the incident recounted by Blair, the on-site sociotechnical subsystem *Syst1.2* did not retain its functional integrity. The cause of the loss of functional integrity was an implementation error—a faulty circuit board. There are numerous ways of rendering circuit boards faulty. Some faults happen spontaneously while others occur due to inadvertent design, manufacturing, installation or maintenance errors. It may be inferred that one of these occurred in the incident recounted by Blair.[21] Such actions may be inadvertent, but some can also be deliberately initiated by a malfeasant intervenor. Once this occurs, these become cybersecurity issues and merit individual consideration.

Circuit board or chip design is a process that usually involves a team. Design errors, inadvertent or deliberate, may be avoided by keeping the design of the chip simple and using formal methods to prove mathematically that the design fulfils the functional requirements. Any attempt to introduce a deliberate design error must somehow circumvent the formal verification. To achieve this result, the formal verification must be manipulated to come up with the result that the design fulfils its requirements, while in actuality the design does not do so. Introducing an error while allowing such 'proof' to be falsely generated is a situation for which it is possible to control using well-exercised human-organizational techniques. One example would be by using separate, independent verification teams and processes. The human-organizational problem of infiltrating each independent verification team and successfully causing a spurious verification in each team may

[18] Blair, 2017 (note 10).

[19] Herley, C., 'Unfalsifiability of security claims', *Proceedings of the National Academy of Sciences of the United States of America*, vol. 113, no. 23 (June 2016) p. 6415–20.

[20] In general engineering terminology, a fault is a system state which would causally engender erroneous behaviour. The erroneous behaviour itself is called a failure. This is the definition of failure in the basic (non-military) electronic/programmable-electronic-system functional-safety standard International Electrotechnical Commission (IEC) 61508. However, IEC 61508-3, Functional safety of electrical/electronic/programmable electronic safety-related systems, 'Part 4: Definitions and abbreviations', 2nd edn, 2010 differs from this. IEC 61508-4:2010 subclause 3.6.1 defines a fault as an 'abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function'. IEC 61508-4:2010 subclause 3.6.4 defines a failure as 'termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required'. See also Blair, 2017 (note 10); Andersen, R. and Sherwin, M. J., 'Nuclear war became more likely this week: here's why', *The Guardian*, 13 Jan. 2018.

[21] Blair, 2017 (note 10).

well be a much harder problem than deliberately introducing a certain kind of error into the design.

Introducing deliberate errors during the manufacturing of a chip would similarly be fraught with organizational problems. If errors are introduced randomly, then it is very likely that such errors would be caught during chip validation. This outcome is 'very likely', however, but not inevitable. This is because it is not possible to test the behaviour of a chip against all possible inputs. Still, validation records show that chip manufacturers are reliable. An error during the installation of a circuit board could cause physical damage to the board resulting in partially different functionality.[22] Connecting the board incorrectly to peripherals could have similar results. Such phenomena are well-controlled through independent validation processes, like with design, as they must guard against inadvertent errors. An error in a circuit board introduced during maintenance, whether inadvertent or deliberate, is controlled for by similar procedures to those for installation.

In sum, the processes that control for inadvertent error in the design, manufacture, installation or maintenance of a circuit board are arguably sufficient to control for deliberate fault introduction. It seems appropriate to suppose that the mechanisms already in place to control for faults in the circuit board lifecycle are sufficient to control for deliberate as well as inadvertent faults. In particular, it seems that there would only be limited scope for achieving such results using so-called new technology, such as deep-learning neural-network (DLNN) technology.

The above discussion goes some way towards substantiating the suggestion that *Syst1.2* is 'fairly robust' in the face of cyberattack. Such an attack would have to focus on specific phases or components of *Syst1.2*. As in the case of a circuit board exhibiting variant functionality, a strengthening of the controls already in place in those phases could well be sufficient to inhibit the introduction of deliberate faults, as well as the inadvertent faults that they already largely inhibit. Other parts of the launch-decision-and-action system appear to be less robust against new technology cyberattack using DLNN technology.

There are three broad ways in which a launch decision could be ill-conceived. First, an attack is in progress and retaliation would not lead to the best possible outcome.[23] The reasoning involved in determining the best possible outcome may be dependent on information supplied externally to the decision maker. This could occur from *Syst3* transforming the information from *(4) Other Environmental Situations*. Such reasoning may be susceptible to loss of information integrity in *Syst3* as well as loss of both functional and information integrity in *(4) Other Environmental Situations*. However, since *(5) Checklist and Procedures/Syst5* is largely static, it is harder to see how functional and information integrity could be lost in this part of the system. It should also be noted that a decision not to launch can be made appropriately, based on information that has retained its integrity.

[22] Driscoll, K. R., 'Murphy was an optimist', Seminar notes, <https://rvs-bi.de/publications/Driscoll-Murphyv19.pdf>.

[23] Blair, 1984 (note 10).

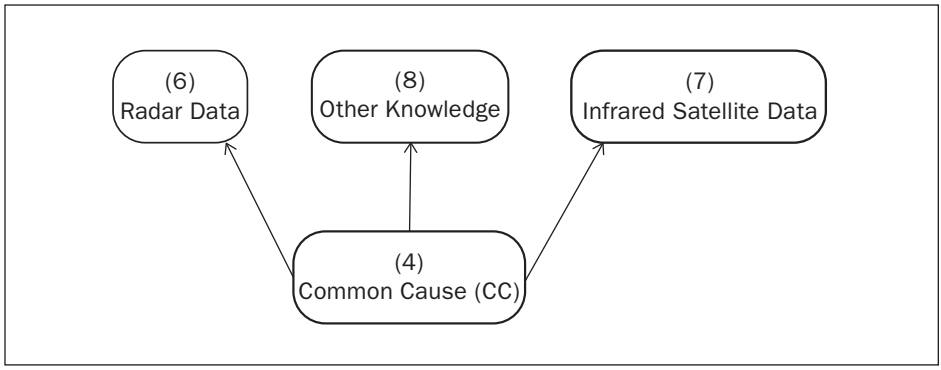

Figure 2.1.3. CCFD illustrating common-cause failure

Source: Author compilation designed by Tim Schürmann using SERAS® YBT4 Beta.

The second way in which a decision not to launch might be made is if the attack is not recognized as an attack and a launch decision therefore not issued due to: (*a*) a loss of integrity (functional and/or informational) in *Syst4*; or (*b*) coordinated loss of integrity in the dual systems comprising *(6) Phenomenology*. This would be a case of common-cause failure, as in figure 2.1.3. However, in the more than half a century that these systems have been in place it is likely that the possibilities for common-cause failure of both parts of the dual phenomenology have been studied in detail and appropriate prophylactic measures introduced. There may be good grounds for constantly reviewing the independence of both channels of the dual phenomenology, but these grounds are independent of how a common-cause failure might occur. If common-cause failures are indeed appropriately inhibited, 'new technology' cyberattacks on the phenomenological channels will by hypothesis not succeed in causing a fail-negative. In this case, the major concern appears to be a loss of integrity in *Syst4* through cyberattack.

The third way in which a launch decision could be ill-conceived is if a decision is made to launch based on 'recognition' of an 'attack' that is not in fact taking place. Assuming that *(6) Phenomenology* is causal in the decision, a false 'recognition' of a phantom attack would involve compromising the information integrity of both channels of the dual phenomenology in a coordinated fashion. This situation received consideration above. It is widely regarded as unrealistic. As above, a loss of integrity in *Syst4*, the causal intermediary system between the facts recognized by the phenomenology and the contribution to a decision, could theoretically result in faulty 'recognition'.

Examples of phenomenological input misleading the military to perceive an impending attack have occurred in both the US and the Russian command.[24] To the knowledge of this author, there has not yet been an incident in which valid warning information was inhibited. The situation in such a common-cause failure of information integrity is illustrated by the CCFD in figure 2.1.3. Note that such a

[24] Sagan (note 10); and *The Economist*, 'Obituary: Stanislav Petrov was declared to have died on September 18', 30 Sep. 2017.

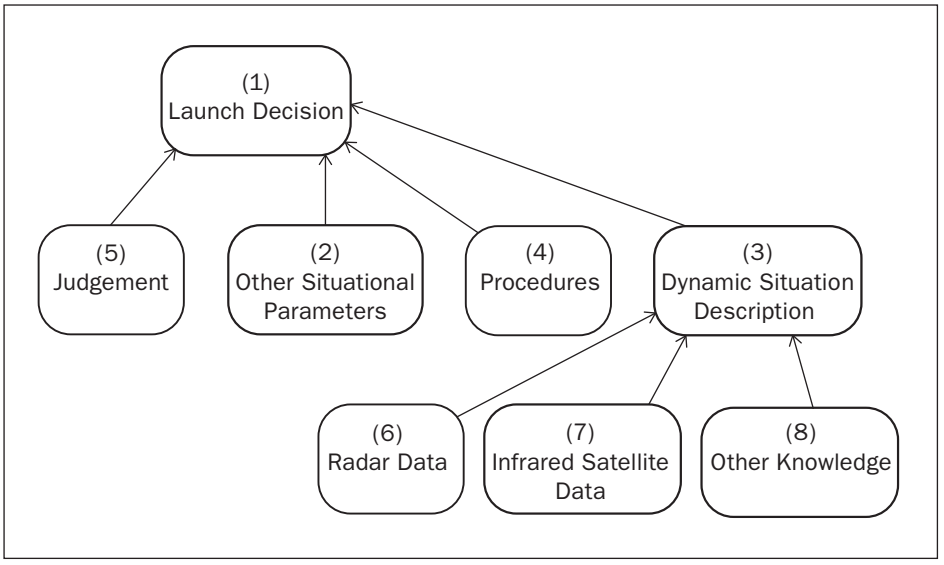

Figure 2.1.4. CCFD showing the information flow into a launch decision

Source: Author compilation designed by Tim Schürmann using SERAS® YBT4 Beta.

common cause would have to affect the subsystems *Syst3* and *Syst4* in figure 2.1.2 in a coordinated fashion. For the reasons of independence adduced above, this would be difficult to achieve.

A final example of the analytical localization of loss of integrity comes from considering in more detail the supporting information flow to a launch decision, as in figure 2.1.4. As noted above, the connections between the informational factors *(2)*, *(3)*, *(4)* and *(1) Launch Decision* is that of desired-to-be-causal rather than truly causal as determined by the counterfactual test. Hence this diagram is a quasi-CCFD. Although dashed lines are not used here, the connections are causal-or-desired-causal and not causal simpliciter.

As noted above, the launch decision is theoretically not required to take available information into account. It is however reasonable to suppose—and indeed expected and anticipated of the decision maker, the US President—that such information from the dual-phenomenological systems, as well as applicable defined procedures, will play a causal role, along with the decision maker's judgement, in a launch decision. These factors are considered below.

1. Figure 2.1.4 shows the dual phenomenology, along with other information. There may be other observers of a potential launch in immediate contact with the Situation Room, such as reconnaissance aircraft gathering telemetry. Such observations are collected under *(8) Other Knowledge*, assembled under the rubric of *(3) Dynamic Situation Description*. It may be theoretically possible for deliberate intervention to cause a failure of information integrity in the dynamic situation description, but only under the condition that

Syst3 and *Syst4* are compromised in a coordinated fashion. It should be possible to inhibit such a coordinated compromise by ensuring that *Syst3* is sufficiently independent of *Syst4*, both physically through sensors and communications and in terms of personnel, and that common causes of loss of integrity of both *Syst3* and *Syst4* are hard or impossible to devise. Such measures would ensure the information integrity of the *(3) Dynamic Situation Description*.

2. The *(5) Judgement* of the decision maker is presumably not influenced by any emerging technology. This analysis distinguishes between judgement as a capability of a human agent, and a discrete judgement that is a result of exercising the judgement capability on given information. The judgement capability is affected by bodily and mental states, and those states can indeed be influenced from outside. But we can presume that, at the time point of a launch/no-launch decision, the decision-maker will be physically protected by attendant personnel from devices that would influence those bodily or mental states; and, in the case of obvious impairment, will be hindered from issuing a call to action. A discrete judgement itself can, of course, be influenced in so far as it is a result of exercising the judgment capability on a collection of information presented, and the information that is presented as input to the judgement can be the result of the use of emerging technology of various sorts. That case, of a judgement which is influenced by information that issues from emerging technology, is covered by the other inputs to the launch decision in Figure 2.1.4.
3. *(4) Procedures* are defined largely statically, as well as independently of the technologies used to implement them. What is required here is to ensure the functional integrity of those procedures, in particular in situations of technology change. This is a matter of defining the functional behaviour of each subsystem and ensuring that under conditions of technology change this functional behaviour is invariant. In other words, this would mean ensuring the functional integrity of the procedures. It is surely relatively easy to devise ways of doing this that are not susceptible to cyberattack.
4. *(2) Other Situational Parameters* is the factor potentially most in need of care and attention. It is possible to envisage new technology such as big-data analytics having an impact. DLNN technology could be applied to various presumed-independent sources of data not derived from traditional sensing technology to enhance the information from the dual phenomenology. If the dual phenomenology maintains information integrity, then such systems are superfluous. As a result, one way of reducing the risk of vulnerabilities in new technology is to enhance the assurance of the information integrity of the dual phenomenology. This is may be difficult, but it is desirable.

Conclusions

This section introduced two notions of system integrity—functional integrity and information integrity—that are more suited to cybersecurity analyses of critical systems than existing notions of integrity in the current standard engineering literature. These notions were applied to an example, the launch system of US ICBMs. It illustrated the use of CCFDs and quasi-CCFDs to describe the causal and desired-causal flows of information and control through the ICBM launch system. Although the quasi-CCFDs were general, the integrity properties of specific subsystems and their effects on the integrity of the overall system could nonetheless be considered at this level of granularity. This process might be called disaggregating integrity requirements. It would be possible to continue the analysis more finely, on finer-grained quasi-CCFDs derived from more detailed system descriptions.

2.2. Defending Japan from offensive cyberattacks

KEIKO KONO[25]

Introduction

There are a number of considerations that merit greater exploration when it comes to the formulation of cybersecurity policy by the Japanese Government. This is particularly the case regarding critical infrastructure protection and potential responses by the government to cyberattacks. When designating critical infrastructure, the Japanese Government identifies 13 sectors: information and communications, finance, aviation, railways, electricity generation and supply, gas, government and administrative services, medical services, water supply, logistics, chemicals, credit card infrastructure and petroleum.

Within this range of sectors, the National Information Security Centre (NISC) is tasked with promoting close cooperation among various actors, from critical infrastructure operators, to a variety of ministries that oversee financial services, internal affairs, health and welfare, economic policy, and transport and infrastructure, to independent agencies that conduct research and development of cyber-technologies and the provision of technical support.[26] These agencies include, but are not limited to, the National Institute of Information and Communications Technology (NICT), the Information Technology Promotion Agency and the Japan Computer Emergency Response Team/Coordination Centre.[27]

This list demonstrates the breadth and complexity of coordination among all of these sectors. While the Japanese Ministry of Defense (MOD) is listed as one of

[25] Dr Keiko Kono is a Senior Fellow at the National Institute for Defence Studies at the Ministry of Defence in Japan.

[26] National Centre of Incident Readiness and Strategy for Cybersecurity, 'Overview of NISC's Activities', <https://www.nisc.go.jp/eng>.

[27] National Institute of Information and Communications Technology (NICT), <https://www.nict.go.jp/en>; Information technology Promotion Agency (IPA), <https://www.ipa.go.jp/index-e.html>; and Japan Computer Emergency Response Team/Coordination Centre, <https://www.jpcert.or.jp/english>.

the bodies concerned, there is no specific mission assigned to the Japan Self-Defense Forces (JSDF) or the MOD's research and development agency, the Acquisition, Technology and Logistics Agency.[28] Instead, the JSDF is only responsible for the protection of its own systems and networks. This section focuses on JSDF missions in cyberspace, and analyses the defence policy and legal challenges facing the Japanese Government in connection with cybersecurity.

Cyber-structure

Japan took a significant step forward in solidifying its cybersecurity framework in 2015 when it established its Cybersecurity Strategy Headquarters (CSHQ), under the Cabinet, according to the Cybersecurity Basic Act.[29] It also created the NISC, which serves as a secretariat for the CSHQ.[30] In contrast to its predecessor, the CSHQ operates as an independent headquarters and works in close cooperation with the National Security Council. In this role, the CSHQ is responsible for preparing the nation's draft cybersecurity strategy. The first strategy was adopted by the Cabinet in September 2015.[31] However, the scope of application of the strategy is only peacetime cyber-incidents. Cyberattacks in wartime are excluded.

Despite its limited scope, the CSHQ is considered Japan's 'control tower' in the cybersecurity field.[32] Within this structure, the NISC has been assigned various tasks, such as performing continuous network monitoring, conducting cybersecurity audits and engaging in analyses of serious incidents. Nonetheless, its responsibilities are limited in scope, covering only central government bodies, incorporated administrative agencies and designated corporations. An example of a designated corporation that would fall under its purview is the Japan Pension Service, which fell victim to a cyberattack in 2015. [33] Other private sector operators do not come under the supervision of the NISC, and it is not able to respond to incidents of cyberattacks that are outside of its jurisdiction.

If, for example, the police identify a cyberattack and the suspect is arrested, it is generally classified as an ordinary crime and the central government is not necessarily required to respond. However, a large-scale cyberattack would constitute a national emergency. According to the government's annual plan on cyber security in 2016, a 'large-scale cyberattack' is defined as a national emergency that has caused, or is likely to cause, material damage to the lives, bodies, property of

[28] Acquisition, Technology and Logistics Agency (ATLA), Japanese Ministry of Defense, <http://www.mod.go.jp/atla/en/index.html>.

[29] Basic Act on Cybersecurity (Act no. 104 of 12 Nov. 2014), Japanese Law Translation Database System website operated by Japan Ministry of Justice.

[30] The predecessor of the NISC dates back to the IT Security Office. It was established within the Cabinet Secretariat in February 2000 and reorganized as the National Information Security Center (NISC) in April 2005.

[31] 'Cabinet Decision on Cybersecurity Strategy', provisional translation, 4 Sep. 2015, <https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>.

[32] Remarks by Prime Minister Shinzo Abe at the first meeting of the Cyber Security Strategy Headquarters, Official Website of the Prime Minister of Japan and His Cabinet, 10 Feb. 2015, <https://japan.kantei.go.jp/97_abe/actions/201502/10article4.html>

[33] '1.25 million affected by Japan pension service hack', *Japan Times*, 1 June 2015.

[Japanese] citizens.[34] In such cases, the government would be expected to play a more proactive role, due to the serious effects on Japanese citizens and critical infrastructure. Government policy distinguishes between two discrete types of large-scale cyberattack: cyber-enabled armed attacks and cyberterrorism. [35] This section focuses on the latter. While Japanese domestic law lacks a concrete definition, the White Paper on Police defines cyberterrorism as a cyberattack on a core system of critical infrastructure.[36] If cyberterrorism occurs in Japan in peacetime, the Deputy Chief Secretary for Crisis Management decides on the necessary initial response and leads the response of government bodies. A Cabinet Task Force takes decisions on the overall response if the initial response is insufficient. Although the National Police Agency is the designated lead agency in responding to cyberterrorism, it would encounter difficulties investigating suspects based in foreign countries. There is no guarantee that assistance or cooperation would be offered by foreign authorities, for example, in the case of a state-sponsored cyberattack such as those allegedly orchestrated by North Korea.

Japan Self-Defense Force

To address some of these threats, in 2014 the MOD established a Cyber Defence Group as a joint unit under the Command, Control, Communications and Computer Systems Command.[37] The commanding officer of the Cyber Defence Group is a Colonel. Although established with only 150 personnel, its staff is expected to grow to up to 1000 in the future.[38] To carry out its mission, the MOD operates two unique information systems: the Defence Information Infrastructure and the Central Command System. These systems constantly monitor all communications by JSDF members and MOD employees.

The Cyber Defence Group only responds to cyber-threats to the JSDF's own network system. Some retired JSDF officers have suggested that, due to the JSDF's dependency on the Nippon Telegraph and Telephone Corporation (NTT), the JSDF would be able under existing laws to protect the NTT network system as part of its asset protection mission (Article 95 of the JSDF Act). However, this remains open to debate. In principle, the JSDF is not permitted to undertake any measures unless provided with the legal authority to do so by domestic legislation.

[34] Japan Cybersecurity Strategic Headquarters, *Cyber Security Annual Plan 2016* (in Japanese), National Center of Incident Readiness and Strategy for Cybersecurity (NISC) website, 31 Aug. 2016, p. 18, <https://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf>. The definition of the 'large-scale cyberattack' derives from the concept of 'an emergency' in the Cabinet Law (Law No. 5 of 22 Jan. 1947, as amended), Article 15 (2).

[35] A classification of a national emergency by the Japanese Government that refers to an armed conflict and cyberterrorism is described on the Japan Cabinet Secretariat website, <http://www.cas.go.jp/jp/gaiyou/jimu/pdf/kinkyu.pdf> (in Japanese).

[36] According to the White Paper on the Police 2016, 'cyberterrorism' is defined as 'an electronic attack on the core systems of a critical infrastructure, or serious failure in the core system of a critical infrastructure that is highly probable to have been caused by an electronic attack', Japan National Police Agency (ed.), *White Paper on Police, 2016*, 2016, p.18 (in Japanese).

[37] 'Regarding Response to Cyber Attacks', *Japan Defense Focus*, no. 42 (2013).

[38] A Cyber Defence Group will be integrated into a newly established joint command over the next few years. The new command is reported to be responsible for outer space and to be headed by the General or flag officers-equivalent JSDF officer. *Yomiuri Shimbun*, 4 Jan. 2018 (in Japanese).

The dominant view among government officials, academics and cyber experts is that the JSDF is neither expected, nor permitted to protect civilian network systems, including critical infrastructure.

In order to clarify some of the legal questions on critical infrastructure protection at the national level, the role of international law will be instrumental to devising clear-cut provisions prohibiting any country from conducting cyberattacks on critical infrastructure. The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) cybersecurity report of 2015 refers to this issue. Paragraph 13(f) provides that 'a State should not conduct or knowingly support ICT [information and communications technologies] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'.[39]

However, this paragraph is listed as a soft law recommendation, which means that it constitutes a voluntary, non-binding norm. This stands in sharp contrast to the Agreement between the Governments of State Members of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring the International Information Security' of 2009.[40] Its Article 4(3) provides that 'each Party shall have an equal right to protect information resources and critically important structures of its state against misuse and unauthorized intervention, including information attacks on them. Each Party shall not carry out such actions in respect to the other Party and assist other Parties in the realization of the above right'. Western nations, including Japan, should explore areas of commonality among themselves, as well as with Russia and China.

Russian scholars from Moscow University have suggested that it is the Russian Government's view that information technologies do not necessarily constitute weapons.[41] At the same time, however, they admitted that information technologies could be used to kill people in the same way as civilian aircraft were used as weapons in the terrorist attacks on the United States on 11 September 2001. [42] This could make it more likely that the international community might be able to agree on basic principles on cybersecurity. Assuming that there is a legally binding agreement that prohibits cyberattacks on critical infrastructure, at least

[39] United Nations, General Assembly, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/770/174, 22 July 2015, para. 13(f).

[40] CIS Legislation, 'Agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security', Unofficial translation, 16 June 2009.

[41] Krutskikh, A. and Streltsov, A., 'International law and the problem of international information security', *International Affairs: A Russian Journal of World Politics, Diplomacy and International Relations*, vol. 60 (2014), pp. 64–76.

[42] Author's meeting with scholars from Moscow University, at the Tokai University 75th Anniversary Memorial International Cyber Security Symposium organized by Strategic Peace and International Affairs Research Institute of Tokai University and the Information Security Institute of Lomonosov Moscow State University on 1 Dec. 2017.

among like-minded countries, the next question would be the consequence of any violation.

More than 30 countries are thought to be acquiring offensive cyber-capabilities.[43] There should be a broad consensus on whether offensive capabilities can be utilized in response to a serious cyberattack in peacetime, or only during wartime. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations provides some guidance on this question.[44] The Tallinn Manual 2.0 opines in its Rule 20 that: 'a state may be entitled to take countermeasures, in response to a breach of an international legal obligation that it is owed by another State'. It further notes in its Rule 26 that: 'a state may act pursuant to the plea of necessity in response to acts' by a non-state actor 'that present a grave and imminent peril . . . to an essential interest when doing so is the sole means of safeguarding it'.[45] This could serve as a foundation for determining the parameters of response.

Challenges

In addressing these developments at the national and international levels, Japan faces a number of challenges. In part, some of these are derived from the government's own defence policy, which is presented as an exclusively national defence-oriented policy. This means that if Japan suffers an armed attack from overseas, the JSDF can respond only to the minimum level necessary for self-defence. This also limits the JSDF to equipping itself with defence capabilities that meet only the minimum requirements necessary for self-defence. As a result, the JSDF cannot acquire offensive weapons such as intercontinental ballistic missiles, long-range strategic bombers and attack aircraft carriers. On the other hand, the government has maintained its policy that it is not necessarily prohibited under the Constitution from using force in self-defence against an aggressor. It has been remaining unequipped with such assets and capabilities.

When it comes to attacking military targets within an aggressor state, Japan has for decades been dependent on US forces. This holds true in the present situation, even in the face of threats from North Korea. This defence policy could also be applied to the way the government responds to serious incidents in peacetime. Given that the government attaches great value to its obligation to respect the sovereignty and territorial integrity of other countries in peacetime, it is highly likely that it would be cautious about the prospect of conducting cyber operations falling short of force to respond to a malicious cyberattack originating from overseas. Therefore, even though an offensive response can be utilized in peacetime under international law, Japan has imposed limitations on itself that prohibit it from engaging in activities that are permitted to other nations.

[43] Lewis, J. A., 'The rationale for offensive cyber capabilities', Center for Strategic and International Studies, 8 June 2016.

[44] North Atlantic Treaty Organization, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to be launched', NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2 Feb. 2017.

[45] Schmitt, M. N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), pp. 111, 135.

Conclusions

If the Japanese Government were to change its defence policy to assign new missions in peacetime to the JSDF in the cyber-domain, it should amend the JSDF law in accordance with its 'positive list', a scheme that is unique to Japanese domestic legislation. In Japan, any government agency—such as the police or the JSDF—is required to seek specific permission to undertake any action. Even if considered justified under the time pressure of an emergency, an operation undertaken without this permission would be deemed unlawful. There is no doubt that if the JSDF were to assume new cyber-missions in peacetime in the future, its operations should not amount to the use of force. From a domestic legal perspective, it should instead remain 'a use of weapons', which falls under law enforcement activity for reasons linked to the law of state responsibility in public international law.

According to Article 50, paragraph (1) (a) of the Articles on State Responsibility drafted by the UN International Law Commission, 'Countermeasures shall not affect the obligations to refrain from the threat or use of force as embodied in the Charter of the United Nations'.[46] This provision is supported by some of the experts who took part in the Tallinn Manual 2.0 project.[47] The majority of the experts on the countermeasures and some of the experts on the plea of necessity argue that a victim state is prohibited from using force when it takes countermeasures or acts pursuant to the plea of necessity in response to a serious cyberattack. A permissible option for a victim state is a cyber-operation below the threshold of a use of force, which means below those that might cause physical destruction and damage to objects, or death or injury of persons.[48]

That said, the concept of a 'use of force' in cyberspace is still unclear. For this reason, a number of definitions need to be better clarified. Among these is the meaning of 'offensive' in cyberspace. If this term covers a broad range of capabilities, it seems likely that the JSDF would be able to conduct certain cyber-operations against an attacking state under its existing defence policy. Thwarting a missile strike by cyber-means, for example, would not cause unnecessary collateral damage to civilian populations and objects.[49] In terms of destructive effect, cyber-capabilities are starkly different from such weapons as intercontinental ballistic missiles and similar platforms. As such, while the Japanese Government's policy on a large-scale cyberattack, especially a cyberattack that falls below the threshold of an armed attack, is lacking. If there were a consensus in the international community that prohibits the use of 'offensive' cyber-capabilities in peacetime among like-minded countries, Japan would be in a better position to assess its own legal structure at the national level.

[46] Crawford, J., *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge: Cambridge University Press, 2002), pp. 288–89.

[47] Schmitt (note 45), pp. 125, 140.

[48] Roscini, M., *Cyber Operations and the Use of Force in International Law* (Oxford University Press: Oxford, 2014), p. 106.

[49] Sanger, D. E. and Broad, W. J., 'Downing North Korean missiles is hard, so the US is experimenting', *New York Times*, 16 Nov. 2017.

3. Private sector and the regional level

3.1. Exploring private sector cybersecurity

SHINICHI YOKOHAMA[1]

Introduction

Over the past three years, the Japanese Government has undertaken a variety of essential initiatives to ensure security in cyberspace. The Basic Law for Cybersecurity was passed by the Japanese Diet in November 2014, and Japan's Cybersecurity Strategy was approved by the Cabinet in 2015.[2] The Fourth Action Plan for Critical Infrastructure Protection was launched in April 2017.[3] These government efforts constitute the foundations for ensuring Japan's cybersecurity.

Despite these advances at the governmental level, most information and communications technology (ICT) assets continue to reside in the private sector. In fact, 90 per cent of Japan's ICT assets are owned by the private sector.[4] Thus, in addition to the foundations established by the government, mature cybersecurity practices at the industry level are needed to achieve national cyber-resiliency. This section covers the progress being made by Japanese industry in its cybersecurity practice.

Practice

To better evaluate the maturity of cybersecurity practice in Japanese industry, the Japanese Government-affiliated Information Technology Promotion Agency (IPA) carried out a global study in the autumn of 2016. The IPA surveyed the cybersecurity practices of companies in Japan, Europe and the United States. It found that 55 per cent of Japanese companies included information technology (IT) systems in their corporate risk assessments, compared to 81 per cent of US firms and 66 per cent of European companies. When asked whether companies performed a damage assessment after a cyber-incident, only 51 per cent of Japanese companies answered in the affirmative, compared with 79 per cent of US and 63 per cent of European companies.[5]

Even more tellingly, 67 per cent of firms have a team to handle cyber-incidents in Japan, compared with 90 per cent of US and 78 per cent of European compa-

[1] Shinichi Yokohama is Head of Cybesecurity Integration at the NTT Corporation in Japan.

[2] Umeda, S., 'Japan: Basic Law for Cybersecurity adopted', *Global Legal Monitor*, Library of Congress, 10 Dec. 2014, <http://www.loc.gov/law/foreign-news/article/japan-cybersecurity-basic-act-adopted>.

[3] Information Security Policy Council, *The Basic Policy of Critical Information Infrastructure Protection*, 3rd edn (Information Security Policy Council, 19 May 2014), <https://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf>.

[4] Research Institute of Economy, Trade and Industry, 'Discussion Papers (Japanese) FY2015', <https://www.rieti.go.jp/en/publications/act_dp_jp2015.html>.

[5] Information Technology Promotion Agency Japan, [Corporate CISO's and CSIRT's Research Status 2017: Investigative report], 13 Apr. 2017 (in Japanese).

nies.[6] Only 63 per cent of companies in Japan had either a full-time or a part-time Chief Information Security Officer (CISO), compared with 95 per cent in the United States and 85 per cent in Europe.[7] There was a full-time CISO in only 28 per cent of Japanese companies.[8] Measured against the 79 per cent of US companies and 67 per cent in Europe, it becomes evident that the cybersecurity practices of Japanese industry are less mature than those of their counterparts. In spite of these lacunae, awareness of the importance of cybersecurity is increasing among business executives in Japan. Despite this fact, many executives currently view cybersecurity as a management issue rather than a technology issue. Thus, it is important to better understand the specific activities of Japanese industry and the progress being made with closing these gaps.

Progress

On 12 December 2017, the Japan Business Federation (*Keidanren*), which is the largest business federation of sectoral trade associations, published its cybersecurity principles.[9] These clearly state that 'self-help' by individual companies should serve as the starting point of cybersecurity. Only after individual companies have engaged in efforts to improve their own standards and conditions can effective collaboration take place. Having passed the litmus test of engaging in self-help and collaborative improvement, these firms would then be eligible for support from the government, not least because industry would then be better positioned to make specific and concrete requests of the government. This industry-driven perspective is a clear shift from the traditional Japanese approach, in which industry tends to be reactive and the government plays the lead role.

At the individual company level, the number of firms that have established Computer Security Incident Response Teams (CSIRTs) is expanding rapidly. The Nippon CSIRT Association (NCA) is a non-profit organization that helps companies to build up these teams.[10] On joining the Nippon CSIRT NCA, companies are offered support to build and strengthen their CSIRTs from other NCA members with more mature practices. Its membership was only around 70 companies in 2014, but had grown significantly to over 270 members as of December 2017. This rapid expansion indicates that Japanese companies are getting serious when it comes to enhancing their cybersecurity practices.

Information Sharing and Analysis Centres (ISACs) have been formed at the sectoral level in Japan. There are currently five, and the financial ISACs, which were established in 2014, demonstrate some of the most mature activities. The telecommunications ISAC was set up in 2002, and was reformed as an ICT ISAC

[6] Information Technology Promotion Agency Japan (note 5).

[7] Information Technology Promotion Agency Japan (note 5).

[8] Information Technology Promotion Agency Japan (note 5).

[9] Japan Business Federation (Keidanren), 'A Call for Reinforcement of Cybersecurity: To Realize Society 5.0', PowerPoint presentation, 12 Dec. 2017, <https://www.keidanren.or.jp/en/policy/2017/103_summary.pdf>; and Japan Business Federation (Keidanren), <http://www.keidanren.or.jp/en>.

[10] Nippon CSIRT Association (NCA), <http://www.nca.gr.jp/en>.

in the spring of 2016 when broadcasters and systems integrator companies were invited to join. Trade ISACs, made up of trading companies, were established in April 2016. Auto ISACs and Japan Electricity ISACs followed in early 2017. Some industries have ISAC-type groups within their trade associations. The chemicals industry is just one example. This proliferation among the various industries in Japan demonstrates the enhanced level of attention being paid to cybersecurity.

Beyond individual sectors, there is also cross-sectoral collaboration. In June 2015, a group of more than 40 companies from various sectors formed the Cross-Sector Forum (CSF) to collaborate on capacity building and information sharing. Members are primarily from different critical infrastructure industries. Most Japanese companies face personnel shortages in their cybersecurity teams. As a result, they have begun joint efforts on talent development. Initially, work was carried out on defining cybersecurity capability profiles, since companies were often faced with vague definitions. A cross-sectoral cyber-talent profile definition reference manual was published in 2016, which has since become the foundation for collaboration among companies on workforce development.[11]

In addition to the domestic activities described above, some companies and sectors have also begun international collaboration. The Financial Services Information Sharing and Analysis Centre (FS-ISAC), which is the global financial industry's resource for cyber- and physical-threat intelligence analysis and sharing, is a sister organization of the FS-ISAC and the two maintain a strong collaborative relationship.[12] The ICT-ISAC hosted two international workshops in 2016 and 2017 with the US-based Information Technology-Information Sharing and Analysis Centre (IT-ISAC), a non-profit, limited liability corporation that serves as a unique and specialized forum for managing risks and corporate IT infrastructure, and the Communications ISAC, an operational arm of the communications sector. The ICT-ISAC also invited Eco International, a German internet industry association, to the international workshop. The ICT-ISAC formed a partnership with the National Council of ISACs in the United States in the autumn of 2017. The Japan Electricity ISAC signed a memorandum of understanding on collaboration with the European Energy ISAC in May 2017. Through these activities, Japanese industry is making step-by-step progress in developing its cybersecurity practices.

Conclusions

Given this sharing of cybersecurity best practices and enhancements at the industry level, Japan is poised to address a number of the cybersecurity challenges that may occur during the Tokyo Olympic and Paralympic Games, which will be held in July 2020. Given current investigations into the technological disruption of the opening ceremony of the Pyeongchang 2018 Winter Olympics, when its press cen-

[11] '『第一期　最終報告書』添付　「人材定義リファレンス」Excel版' ['Personnel Declaration' added to the 'First Phase Final Report' Excel Version], 14 Sep. 2016, <http://cyber-risk.or.jp/cric-csf/jinzai_reference_2016.html>.

[12] Financial Services Information Sharing and Analysis Centre, <https://www.fsisac.com>.

tre and websites had to be shut down for an extended period, the potential for a cyber-disruption cannot be ignored.[13] For Japan, there will be full-scale preparations to ensure cybersecurity at all the events in Tokyo. Wide-scale cooperation will be required from industry to ensure security at the event. Since cyberspace lacks borders, regional and international collaboration will also be needed. Nonetheless, such preparations must not be limited to the seven-week Olympic and Paralympic period. The ultimate goal, beyond 2020, will be to establish cyber-resiliency within Japanese society. In the next few years, there will be a unique window of opportunity and momentum to achieve this goal, particularly as Japan makes plans to host two of the most widely attended and watched global sporting events. Japan's private sector will be at the forefront of this activity.

3.2. Constructing the EU's cybersecurity strategy

SARAH BACKMAN[14]

Introduction

Digital developments in modern society have been explosive, enhancing global ICT dependence in unforeseen ways. The digital revolution has removed borders that were formerly obstacles to global communications, collaboration and trade. At the same time, this rapid digital development, driven by the relatively low costs of innovation, has resulted in extensive security gaps and threats at all levels of society. Collecting cyber-threat data from all over the world, Symantec noted in 2016 that cyber-threats have been constantly increasing for a number of years, and cyberattacks have been breaking records year after year. Symantec's report noted that 'perhaps what is most remarkable is that these numbers no longer surprise us. As real life and online become indistinguishable from each other, cybercrime has become a part of our daily lives. Attacks against businesses and nations hit the headlines with such regularity that [we have] become numb to the sheer volume and acceleration of cyber-threats'.[15]

Several real-life incidents have demonstrated how vulnerable modern society is to cyberattacks. Extensive security gaps at all levels of society are continuously exploited for a variety of purposes that include financial gain, political influence, hacktivism, espionage, industrial espionage and even cyberwarfare. Among the examples are the distributed denial of service (DDoS) attacks on Estonian Government websites in 2007, the Zeus 2009 banking Trojan that stole banking information, the Stuxnet worm in 2010 that attacked Iranian nuclear centrifuges, the German steel mill attack of 2014, the attacks on the power grid in Ukraine in 2015 and the Wannacry ransomware attacks on hospitals in 2017. In responding to this varied threat landscape, the development of European cybersecurity measures

[13] Ingle, S., 'Winter Olympics investigating if technical problems were cyber-attack', *The Guardian*, 10 Feb. 2018.

[14] Sarah Backman is a consultant with Secana Cybersecurity in Sweden.

[15] Symantec, *Symantec Internet Security Threat Report*, vol. 21 (Apr. 2016), p. 5.

has been swift, particularly since the 2013 publication of the first EU cybersecurity strategy.[16] The EU cybersecurity strategy identifies three main 'pillars' of cybersecurity: societal security or network and information security (NIS), cybercrime prevention and cyber-defence. Although interconnected and overlapping, each pillar has specific features.

Features

The European Cybercrime Centre (EC3) plays a major role in cybercrime prevention, engaging in activities such as operational coordination among member states, awareness raising initiatives, early warning notifications, threat assessments and decision-making support with cybercrime prevention and management.[17] The two dominant malware threats encountered by EU law enforcement are ransomware and information theft via malware. Social engineering is a common component of these attacks, since the human component is often the weakest link in the chain. Within the pillar of cybercrime, attacks targeting individuals are common and can include identity theft, sexual exploitation, payment fraud and stolen personal information. An important measure within this pillar is the EU General Data Protection Regulation (GDPR), which enters into force in May 2018 and seeks to strengthen the right to privacy of individuals and the management of personal information.[18] The European Union Agency for Network and Information Security (ENISA) is an important actor in the societal security or NIS pillar, conducting pan-European cyber-crisis exercises (Cyber Europe), enhancing cybersecurity awareness, supporting member states as they build capacity and promoting collaboration and information sharing.[19]

Recognizing that 'past efforts have been on too small a scale and too fragmented' and that 'the voluntary nature of past efforts [left] many gaps in our overall cybersecurity', the ENISA proposed an NIS directive in 2013 along with its cybersecurity strategy.[20] This was adopted in its final form in July 2016 and will be implemented in member states' legal frameworks in May 2018. The directive aims to enhance the common and individual cybersecurity capacities of the member states and to enhance the general level of information security within critical infrastructure sectors. It entails an obligation on member states to establish national cybersecurity authorities and to create their own national cybersecurity strategies. It further requires operators of critical societal sectors such as transport, finance and energy, as well as digital service providers, to achieve a

[16] EPSC, 'Building an effective European cyber shield: Taking EU cooperation to the next level', *Strategic Notes* no. 24 (8 May 2017).

[17] Europol, 'European Cybercrime Centre: EC3, Combating crime in a digital age' [n.d.].

[18] European Commission, General Data Protection Regulation (GDPR), Press release, Brussels, 24 Jan. 2018.

[19] European Commission, 'State of the Union 2017: The Commission scales up its response to cyber-attacks', Fact sheet, Brussels, 19 Sep. 2017.

[20] European Commission, 'Proposed Directive on network and information security: Frequently asked questions', Press release, Brussels, 7 Feb. 2013.

minimum level of cybersecurity and to report cyber-incidents.[21] The NIS directive has established measures such as new venues of cooperation and information sharing on cyber incidents. One such example is the Computer Security Incident Response Team (CSIRT).

Among the pillars, the one governing cyber-defence is the least developed, since it remains a sensitive area for EU involvement. Nonetheless, several initiatives have been initiated to enhance collaborative capacities and to exchange instruments between the EU and the North Atlantic Treaty Organization (NATO). One of these is the Technical Arrangement on Cyber Defence, which was concluded between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU) for exchanging information and sharing best practices between emergency response teams.[22] The EU also aims to enhance interoperability among its member states through training and education. The European Defence Agency and European External Action Service are two important actors within this pillar.

Conclusions

The publication of the EU cybersecurity strategy and the NIS directive are among a range of approaches that have emerged following a number of successful cyber-attacks on an ever more digitalized society. The three cybersecurity pillars of societal security or NIS, cybercrime prevention and cyber-defence may overlap but are still guided by their own challenges, response actors and measures. While the EU has come a long way in its development of these measures, it continues to face a wide range of challenges. Information sharing remains a hurdle as it tests the willingness of EU member states to share sensitive cybersecurity information. Furthermore, the EU is beset by its need to balance sovereignty and common responses through horizontal and vertical collaboration at the technical and strategic levels. Finally, communication problems continue to afflict member states, which face differences in both terminology and technology.

Overall, digital development has had sizeable advantages for individuals and societies. It has allowed societies to innovate, connect, collaborate and develop in ways that were not previously possible. The 'digital revolution' has succeeded in bringing the world closer together, increasing freedom and speeding societal development. However, much like other revolutionary technologies such as road and air travel, the need for security measures and regulation has become increasingly apparent. In the cyberspace realm, the EU is increasingly aware of the need for common regulations, security measures and enhanced end-user knowledge to combat the proliferation of cyberattacks and to foster greater information sharing and connectivity among its members.

[21] Council of the European Union, 'EU-wide cybersecurity rules adopted by the Council', Press release, 17 May 2016.

[22] North Atlantic Treaty Organization, 'NATO and the European Union enhance cyber defence cooperation', Press release, 10 Feb. 2016.

4. Legal frameworks and the international level

4.1. Laying the groundwork for cyber-norms

GARY BROWN[1]

Introduction

Despite the commonly recognized threat of cyber-aggression against national critical infrastructure worldwide, little progress has been made in using law and policy to address this issue.[2] The problem is so challenging that it is possible no significant steps will be taken until a cyberattack causes large-scale destruction. Rather than submitting to the inevitability of this prospect, a few states and international organizations, such as the United Nations, continue to search for ways to avoid disaster. Progress in this arena has proved elusive, but the most promising approach seems to be developing limited international agreements and international norms of behaviour.

International norms typically develop through years of state practice in an area, through repeated trial and error, as states reach accommodations with each other and eventually determine the best approach to avoiding conflict. Over time, these practices can develop into international law. Unlike national activities in more traditional areas of international relations, state practice in cyberspace is generally secret and undisclosed. While there might be speculation about the perpetrator of a cyber-incident, unless states publicly take responsibility for an action or event, there is no foundation for developing patterns of state practice, which inhibits the development of international norms. Even public statements have done little to advance cyber-rules, because states have generally under-reacted to cyber-allegations. This is perhaps in large part because attribution is difficult, embarrassment levels are high and the methods that disclose system compromises are often sensitive.

Norms

The absence of public practice has led to unfortunate efforts by international organizations and states to negotiate 'norms'. This approach is arguably oxymoronic. At the heart of a norm lies informal state agreement and practices that have accumulated over time. Negotiations lead to formal and enforceable international

[1] Colonel (retd) Gary Brown, Air Force, was the first Senior Legal Counsel, US Cyber Command. The views expressed are those of the author and do not necessarily represent the views of the US Department of Defense.

[2] The US defines critical infrastructure sectors as 'the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety'. Sixteen broad sectors are identified, including nuclear power, transportation, finance and health care. US Department of Homeland Security (DHS), *What Is Critical Infrastructure?* (DHS: Washington, DC, 2017). Houck, C., 'OK, say someone hacks into the US power grid: Then what?', Nextgov, 7 Dec. 2017.

agreements, while norms are informal and unenforceable standards of behaviour. Nonetheless, efforts to craft some standards continue. For example, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has provided reason for optimism.

Earlier generations of the UN GGE made incremental progress towards developing standards on which states could agree. For example, the 2015 UN GGE report lists several recommendations for 'new norms and principles', such as that states should not allow their territory to be used for internationally wrongful cyber-acts, should not conduct or support cyber-activity that intentionally damages critical infrastructure and should not conduct or support activity to harm the information systems of another state's emergency response teams, including CERT and CSIRTs.[3] The UN GGE took a practical approach that sought basic common ground on which to build. These suggested norms seem logical and straightforward but, much like everything related to cyberspace, they are difficult to apply.

For example, the norm to avoid targeting CERTs is premised on avoiding them because they serve no function other than to maintain the internet's functionality, which benefits everyone. Muddling that position, however, is the complex role of CERTs. They often serve a variety of functions in different states, providing information to law enforcement and intelligence agencies, for example, in addition to keeping the internet up and running. These additional roles make them a valid and attractive target for adversary states, which means placing them 'off limits' to cyberattack is somewhat unrealistic. Moreover, the most recent, fifth iteration of the UN GGE concluded rather ingloriously. Specifically, it rejected the conclusions reached by previous UN GGEs, and declined to address the right to cyberspace self-defence and engagement in cyber-countermeasures. It even failed to agree that International Humanitarian Law applies in cyberspace.[4] More generally, the process failed partly because states continue to avoid placing their cyber-strengths on the table for negotiation.

For example, China is reputed to be particularly skilled at corporate espionage and internal information control, while the United States is reportedly adept at national security espionage and Russia allegedly excels in information manipulation, in particular of external information flows.[5] Developing states see cyberspace as a relatively fast and inexpensive way to level the playing field with the traditional powers. As might be expected, states are interested in maximizing flexibility in their areas of cyber-strength, while being willing to limit legal options

[3] North Atlantic Treaty Organization, Cooperative Cyber Defence Centre of Excellence, '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law', 31 Aug. 2015.

[4] Schmitt, M. and Vihul, L., 'International cyber law politicized: The UN GGE's failure to advance cyber norms', Just Security, 30 June 2017.

[5] Segal, A., 'How China is preparing for cyberwar', *Christian Science Monitor*, 20 Mar. 2017; Poulsen, K., 'Surprise! America already has a Manhattan Project for developing cyber attacks', *Wired*, 18 Feb. 2015; and Sanovich, S., 'Computational propaganda in Russia: The origins of digital misinformation', *Working Paper 2017.3* (Computational Propaganda Research Project, University of Oxford: Oxford, Mar. 2017).

in areas where their rivals are stronger. Because these areas do not align, there is little common ground between states and reaching consensus on appropriate norms is difficult. The situation leaves critical infrastructure at risk from all types of espionage, which could result in inadvertent damage and harm to civilian populations, as well as unintentional triggering or escalation of interstate conflict.

Conclusions

Given these challenges, when seeking means to develop norms, perhaps one of the best initial steps would be to concentrate international efforts on repeated state practice and working towards bilateral agreements between allies. If enough states partner with each other to agree on certain norms of behaviour, common elements from several bilateral agreements could serve as a starting point for the development of international norms. Despite the obstacles, international norms may well offer the best path to stability and the protection of critical infrastructure. Importantly, states cannot merely sit back and do nothing because inaction also creates norms and there is a global trend for cyberattacks to increase in severity.[6] To mitigate and in some cases even forestall these developments, responsible states should take action now to address these issues before they spiral out of control.

4.2. Building international consensus in cyberspace

ENEKIN TIKK[7]

Introduction

For over a decade, it has been acknowledged that critical infrastructure is one of the more problematic areas in the context of state use of information and communications technologies (ICTs). In a submission to the United Nations in 2000, Poland recognized the potential threat from unauthorized interference with the integrity of information-based critical infrastructure.[8] Since that time, Germany has observed that 'process control systems for critical infrastructures have proven particularly vulnerable to malicious information and communications technology operations', such that 'the risks of uncontrollable collateral damage on a global scale are high, including the infection of industrial control systems with potentially physical destructive effects'.[9] Most recently, Ukraine has been the victim of a marked rise in cyberattacks against critical national infrastructure, which cause damage to states through the distortion of important information and the

[6] Graff, G. M., 'How a dorm room Minecraft scam brought down the internet', *Wired*, 13 Dec. 2017.

[7] Dr Eneken Tikk is Head of Strategy and Power Studies at the Cyber Policy Institute in Jyväskylä, Finland.

[8] United Nations, General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/55/140/Add.1, 3 Oct. 2000, p. 2.

[9] United Nations, General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/68/156/Add.1, 9 Sep. 2013, p. 5.

disruption of production processes at factories, interrupting the supply of utilities and energy, and disrupting transport systems.[10] Ukraine faced two of the more prominent cyberattacks in recent history when attacks in 2015 and 2016 targeted its power grid.

In spite of these common concerns, the no-consensus outcome of the fifth round of the UN GGE in 2017 elicited questions about the value of expert recommendations and the working format.[11] States remain divided over military threats to critical infrastructure. Some of this may be attributable to the differences in definitions of informational versus kinetic cyber-threats. In 2001, Russia devoted a whole chapter of its UN submission to the topic of the deliberate use of information to influence another state's 'vital structures'.[12] Russia has warned that disruptions of the normal functioning of state systems and institutions would be viewed as constituting a direct threat to national security.[13] Russia has listed vital systems such as computerized power control systems, for instance in the country's life support infrastructure and nuclear power stations, as vital systems, as well as national defence systems and the communication, control and transportation systems of services dedicated to saving lives and dealing with natural disasters or other emergency situations.[14] The United States has noted in its own official documents submitted to the UN that the threats brought about by the convergence between ICT, the internet and other infrastructure provide unprecedented opportunities to cripple telecommunications, electricity generation and supply, pipelines and refineries, financial networks and other critical infrastructure.[15]

Deliberations

Thus, whether due to cyberattacks on information or hardware, the UN GGE concluded in 2010 that the growing use of ICTs in critical infrastructure creates new vulnerabilities and opportunities for disruption.[16] In an early example of consensus regarding common threats to the ICT sphere, experts recommended further dialogue among states to reduce risk and to protect critical national and international infrastructure.[17] The UN GGE called for capacity building to assist developing countries in their efforts to enhance the security of their critical national information infrastructure.[18] It also invited states to discuss norms pertaining to state use of ICTs to reduce collective risk and protect critical national and inter-

[10] United Nations, General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/67/167, 23 July 2012, p. 16.

[11] Tikk, E. and Kerttunen, M., 'The alleged demise of the UN GGE: An autopsy and eulogy'.

[12] United Nations, General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/56/164/Add.1, 3 Oct. 2001, pp. 2–3.

[13] United Nations (note 8).

[14] United Nations, General Assembly (note 12), pp. 2–3.

[15] United Nations, General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/66/152, 15 July 2011, p. 15.

[16] United Nations, General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/65/201, 30 July 2010, p. 2.

[17] United Nations, General Assembly (note 16), p. 2.

[18] United Nations, General Assembly (note 16), p. 8, para. 17.

national infrastructure.[19] In 2013, the UN GGE report added to the urgency by noting that threats to national infrastructure had grown more acute and incidents more damaging, particularly given the expanding use of ICTs in critical infrastructure and industrial control systems, creating new possibilities for disruption.[20] To increase confidence in this context, experts called for increased cooperation on and support for bilateral, regional, multilateral and international capacity-building efforts to secure ICT use and infrastructure.[21] The theme was elevated further in the 2015 report, in which experts concluded that the most harmful attacks using ICTs were those targeted at the critical infrastructure and associated information systems of a state.[22] The UN GGE viewed the risk of harmful ICT attacks against critical infrastructure as 'both real and serious'.[23]

Accordingly, and echoing the recommendations made by several states in their written contributions, the UN GGE made several recommendations on improving the security of critical infrastructure. It agreed with Germany that states should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.[24] However, in spite of this seeming agreement, the UN GGE did not agree to make this as a binding obligation in international law. Instead, it referred to it as a voluntary, non-binding commitment. Furthermore, the UN GGE recommended that states take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructure, and other relevant resolutions.[25] It also called on states to respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts.

To this end, the UN GGE recommended confidence-building measures to address critical infrastructure security. It concluded that states should voluntarily provide their national views on the categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies on the protection of data and ICT-enabled infrastructure.[26] States were called on to seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. Such measures might include:

[19] United Nations, General Assembly (note 16), p. 8, para. 18 (i).

[20] United Nations, General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/68/98, 24 June 2013, p. 7, para. 9.

[21] United Nations, General Assembly (note 20), p. 10, para. 32 (a).

[22] United Nations, General Assembly, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/770/174, 22 July 2015, p. 6, para. 5.

[23] United Nations, General Assembly (note 22), p. 6, para. 5.

[24] United Nations, General Assembly (note 22), p. 8, para. 17 (f).

[25] United Nations, General Assembly (note 22), p. 8, para. 17 (g).

[26] United Nations, General Assembly (note 22), p. 8, para. 17 (d).

> '16 (d) i. A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;
>
> ii. The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;
>
> iii. The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;
>
> iv. The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents'.[27]

Somewhat surprisingly given that there were no national submissions on the issue, the UN GGE has suggested that states might wish to consider including national CERTs and/or CSIRTs within their definition of critical infrastructure.[28] Concluding that a lack of capacity can make the citizens and critical infrastructure of a state vulnerable, the UN GGE recalled resolution General Assembly Resolution 64/211. 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures'.[29]

With reference to international law, the experts emphasized that 'States have jurisdiction over the ICT infrastructure located within their territory'.[30] Nonetheless the UN GGE had reservations about the conditions under which states may be held responsible for ICT activity that is launched or otherwise originated from their territory or ICT infrastructure, 'States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State'.[31] The expert group also noted that further work is needed to achieve 'increased cooperation at the regional and multilateral levels to foster common understandings on the . . . security of ICT-enabled critical infrastructure.[32]

Conclusions

In spite of the tendency to view the lack of consensus at the end of the 2017 UN GGE meeting as a failure, there have been areas of progress on which the process can build. Despite fundamental differences among states about several principal issues, such as the legally binding nature of due diligence, the emphasis on national versus international efforts and the nature of the threat, the experts

[27] United Nations, General Assembly (note 22), p. 8, para. 16 i–iv.

[28] United Nations, General Assembly (note 22), p. 10, para. 17 (c).

[29] United Nations, General Assembly (note 22), p. 10, paras 19 and 21; and General Assembly Resolution 64/211. 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures', 21 Dec. 2009.

[30] United Nations, General Assembly (note 22), p. 12, para. 27.

[31] United Nations, General Assembly (note 22), p. 13, para. 28 (f).

[32] United Nations, General Assembly (note 22), p. 13, para. 30 (b).

still managed to find common ground and surprising coherence in their recommendations. The meeting also provided a checklist for states seeking to consider cross-border threats to their critical infrastructure. While some countries regard the protection of critical infrastructure as primarily a national responsibility, the majority seem to agree that, at a minimum, exchanges of best practices and national experience are necessary to provide effective guarantees against critical infrastructure-related cyberattacks. Thus, relevant exchanges of information and assistance constitute increased expectations in international cyber-affairs.

Effective protection of critical infrastructure remains empirically demanding. The lack of conceptual and definitional clarity leaves states largely on their own when deciding what merits protection as critical infrastructure, in particular with regard to the threats resulting from the development and use of ICT. Given the widely acknowledged interconnectivity of systems and services, the critical infrastructure dialogue should also cover cross-border aspects. For instance, the Global Commission on the Stability of Cyberspace has raised the need to protect the functionality of the internet.[33] In addition to identifying critical objects, sectors, functions and services, states are expected to create working mechanisms for assessing and mitigating the threats that the development and use of ICT raise for such infrastructure.

The UN GGE discourse highlights several threat factors and actors. However, the UN GGE remained split on the relative role of critical infrastructure-related threats in international cybersecurity. At the same time, the UN GGE's focus, by definition, cannot be expected to fully extend to national best practices and to all the modalities for national implementation of its guidance. Similarly, its guidance on critical infrastructure protection cannot be considered exhaustive and comprehensive, as it primarily seeks to address those aspects of critical infrastructure that are relevant to international peace and security.

Finally, the UN GGE cannot be expected to provide extensive guidance to states on the relationship between the state and the private sector. This applies to the interactions between authority, responsibility, coordination and appropriate public–private partnerships, as well as the organization-level routines for securing critical infrastructure objects. For this kind of guidance, states could examine the national contributions made in the context of the global culture of cybersecurity in the Second Committee. Overall, the international community remains divided over whether the threats to national and international critical infrastructure resulting from the development and use of ICTs are of a military nature and of direct relevance to international peace and security. However, it seems to be the majority view that the topic of critical infrastructure protection merits further discussion in the First Committee. This means that in terms of longer term measures to address cyberattacks on critical infrastructure, there is enough common interest and momentum to compel states to continue to engage in efforts to build consensus.

[33] Global Commission on the Stability of Cyberspace, 'Call to protect the public core of the internet', 21 Nov. 2017.

5. Conclusions

Across the spectrum of national, regional and international developments, this volume has sought to provide nuance to the discussion of cybersecurity and critical infrastructure. Specific examples of system engineering, industry developments and legal frameworks highlight the complexity of building a static framework or format for cyber-standards and best practices. While progress has been made in terms of Japan's building of organizations to monitor and respond to cyberattacks, ongoing questions of jurisdiction at the national level hinder the ability to coordinate both preparation and response. Furthermore, long-standing constraints on the role of the JSDF have led to questions about the role it could play outside of its narrowly defined parameters in the event of a large-scale, offensive cyber-attack against Japan's critical infrastructure. At the ministerial and industrial levels, expanded assistance with forestalling and navigating cyber-incidents from the National Information Security Centre has provided a degree of reassurance. However, the fact that more than 90 per cent of vulnerable ICT infrastructure is spread throughout disparate companies and firms highlights the difficulties of integrating national standards and responses across different jurisdictions and the private sector.

When it comes to regional coordination, the EU poses a unique challenge in that it is a body of countries that are still struggling to integrate both their regulatory frameworks and their information sharing practices. This places in high-relief the inherent complexity of coordinating among even like-minded countries to define and respond to cyber-incidents. Moreover, expanded regulatory priorities on information security combined with efforts to enhance information sharing may produce future tensions. As one participant in the workshop noted, a preponderance of regulations and checklists does not necessarily lead to greater protection for critical infrastructure, particularly if basic cyber-hygiene at individual facilities remains weak. The case of system integrity further demonstrates this dilemma as the end-user inserted into the operation of critical infrastructure is not only one of the weakest links in the cybersecurity chain, but also complicates efforts to determine the integrity of a system.

Many of the national and regional issues mentioned above become even more stark at the international level, as countries still tend towards a sovereignty-based view of cyberspace. Navigating the varied stances among these countries will be essential to reaching comity on the risks of cyberattacks to critical infrastructure. Nonetheless, the lack of consensus at the UN GGE in 2017 demonstrates that countries remain divided even on the most basic tenets of International Humanitarian Law and the nature of information security and cybersecurity. To remedy this, greater efforts among like-minded states to work at the bilateral and mini-lateral levels could serve as a foundation for building a series of norms that could be incrementally integrated at the international level. Such coalition building, however, could also lead to greater fragmentation by region or technical capacity. Given the comparative nascence of cyber frameworks at the national and regional

levels, the integration of norms at the international level is likely to depend on the establishment of these norms at home.

Unfortunately, as aptly pointed out by one of the workshop participants, the cyberspace domain may have to wait for a large-scale cyberattack on critical infrastructure before an impetus for sweeping change emerges. As this volume indicates, resiliency in terms of cybersecurity and critical infrastructure must be addressed at the levels of system integrity, private sector engagement, national frameworks, regional integration and international norms. The lack of consensus, even among like-minded states, in terms of definitions and frameworks indicates that these levels are likely to remain disconnected for the foreseeable future. Faced with this fragmentation, providing the opportunity for like-minded and even dissenting states' academic, political, military, technical and legal experts to assemble and to discuss their respective policies on cybersecurity and critical infrastructure provides a baseline to facilitate official-level talks.