Smart Innovation, Systems and Technologies 138

Denis B. Solovev *Editor*

Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and Production

Proceeding of the International Science and Technology Conference "FarEastCon-2018" Volume 1

KES International

Springer

Smart Innovation, Systems and Technologies

Volume 138

The Smart Innovation, Systems and Technologies book series encompasses the topics of knowledge, intelligence, innovation and sustainability. The aim of the series is to make available a platform for the publication of books on all aspects of single and multi-disciplinary research on these themes in order to make the latest results available in a readily-accessible form. Volumes on interdisciplinary research combining two or more of these areas is particularly sought.

The series covers systems and paradigms that employ knowledge and intelligence in a broad sense. Its scope is systems having embedded knowledge and intelligence, which may be applied to the solution of world problems in industry, the environment and the community. It also focusses on the knowledge-transfer methodologies and innovation strategies employed to make this happen effectively. The combination of intelligent systems tools and a broad range of applications introduces a need for a synergy of disciplines from science, technology, business and the humanities. The series will include conference proceedings, edited collections, monographs, handbooks, reference books, and other relevant types of book in areas of science and technology where smart systems and technologies can offer innovative solutions.

High quality content is an essential feature for all book proposals accepted for the series. It is expected that editors of all accepted volumes will ensure that contributions are subjected to an appropriate level of reviewing process and adhere to KES quality principles.

**** Indexing: The books of this series are submitted to ISI Proceedings, EI-Compendex, SCOPUS, Google Scholar and Springerlink ****

More information about this series at http://www.springer.com/series/8767

Denis B. Solovev
Editor

Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and Production

Proceeding of the International Science and Technology Conference "FarEastCon-2018" Volume 1

Springer

Editor
Denis B. Solovev
Department of Innovatics,
Engineering School
Far Eastern Federal University (FEFU)
Vladivostok, Russia

ISSN 2190-3018 ISSN 2190-3026 (electronic)
Smart Innovation, Systems and Technologies
ISBN 978-3-030-15576-6 ISBN 978-3-030-15577-3 (eBook)
https://doi.org/10.1007/978-3-030-15577-3

Library of Congress Control Number: 2019934741

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection

E. Gorian(✉)

Vladivostok State University of Economics and Service,
41, Gogol Street, Vladivostok 690014, Russian Federation
ella.goryan@vvsu.ru

Abstract. National mechanisms of critical information infrastructure (CII) protection differ depending on the information assets, authorities' powers, methods of regulation, etc. Singapore implements the state-driven approach for CII protection that is balanced and calibrated in order to harmonize the efficient powers of authorities with the burdens imposed on IT industry parties. Singapore's Cybersecurity Act 2018 (CSA) establishes a solid and precise framework for the CII protection specifying three core aspects: constant cooperation of public authorities and private sector in envisaging a CII system; broad authorities for prevention, management and response to cybersecurity threats and incidents in Singapore, and compulsory licensing of cybersecurity services. It emphasizes compliance with promulgated codes of practice and expresses designation of CII and cybersecurity threats. The distinctive feature of the act is its significant reduction of the compliance burden on cybersecurity professionals and CII owners. As for the CII protection it's important that computer systems in the supply chain supporting the operation of a CII (i.e. data centre owners and cloud services operators) will not be designated as CIIs. Thus the CSA illustrates the narrow approach of law makers in envisaging its jurisdiction – it implies just CII owners and not any network operators. Singapore is a first jurisdiction in South-East region that has developed its cybersecurity legislation to impose requirements on certain businesses to implement protections against cybersecurity risks into their computer systems.

Keywords: Cybersecurity · Critical information infrastructure · CII protection · Jurisdiction

1 Introduction

Communication networks are a significant element of the modern life. The vast majority of liaisons within the communities, the business environment, the state or the international community are allocated exclusively in such networks. They are the pillars of the information society and an essential part of the single digital market. Some of them are critically important for the national security reasons as they provide vitally important resources or support their movement. Such information infrastructures are critical for the people's convenience and even existence [1] and therefore they are

D. B. Solovev (Ed.): FarEastCon 2018, SIST 138, pp. 1–9, 2020.
https://doi.org/10.1007/978-3-030-15577-3_1

considered as critical information infrastructures (CIIs). CIIs are the frequent targets for cyber-attacks so the states try to cope with these threats and to search for the adequate structures and processes that could optimally tackle the new cyber risk while protecting core civil rights [2]. In general the situation with CIIs protection on the national level sounds like satisfying. The main trend of delegating responsibility to cyber security authorities, emergency agencies or national regulators which are responsible for operational tasks is being observed. Many of those authorities are responsible for additional tasks on the strategic or political level, such as the development of strategy papers, supervision of the national computer security incident response team or the proposing legislation. Still the half of the national mechanisms have established institutionalized forms of cooperation in forms of public-private partnerships in spite of the fact that the private sector bears responsibility for ensuring network resilience and moreover it participates in the regulation of national information security by providing technical expertise [3]. For all states the critical sectors with the strongest regulations are the telecommunications, finance and energy sectors. Not all the states conduct a risk assessment on a national level. They imply the policy of imposing the responsibility for the risk assessment on sector-specific agencies or on the individual operators [4]. Therefore national standards of CIIs protection differ from the simplest to the advanced ones. It is a fact that states that play a leading role in international economic relations and digital markets are constantly developing their national standards of CIIs protection in order to ensure not only the interior business and community liaisons but also a global supply chain.

Being a most connected nation in a world, Singapore is also an international centre of exchange and commerce. That makes it a perfect target to cyber threats and attacks with more severe consequences for the public order and economics of Singapore then for any other state. Therefore Singapore legislature presented a Cybersecurity Act (CSA) in 2018 following the harsh and productive public debates with private sector involved. It is considered as a new generation standard for protection of CIIs that makes it an object of close attention of professionals from different spheres.

2 Methodology and Literature Review

Please note that the first paragraph of a section or subsection is not indented. The first The methodology for this study comprises of two groups of methods: the general scientific ones (system-structural, formal-logical and hermeneutical methods) and the special legal methods of cognition (comparative legal analyses and formal-legal method). In order to obtain the most reliable scientific results they were used in complex.

CII protection system demands including stakeholders from the public and the private sectors. In many states CII is operated by private entities which are connected internationally through the participation in the entire supply chain. Häyhtiö and Zaerens (Häyhtiö and Zaerens 2017) introduce a management model which enables a network wide protection for critical infrastructure in a contractual environment between the actors with different business domains and functions in a supply chain [5]. Such management model can be used to assess financial differences between centralized and decentralized protection of critical infrastructure.

Because of its operative capacity, the private sector has come to be understood as the expert in network and information systems security, whose knowledge is crucial for the regulation of the field. Farrand and Carrapico (Farrand and Carrapico 2018) identify the shifting role of the private sector in the CII from one of a victim in need of protection in the first phase, to a commercial actor bearing responsibility for ensuring network resilience in the second, to an active policy shaper in the third, participating in the regulation of NIS by providing technical expertise [3].

Every state develops its own model for CII protection (the physical one primarily) and it requires the methodological approaches to be used. It helps to estimate hazards and threats to the infrastructure objects. Bobro (Bobro 2018) emphasizes the necessity of all hazards approach (considering the threats of any origin and directionality). The threats model must use not only the violator's model, but also the object's model and the model of socio-political situation [6].

The nature of cyberspace and its constant evolution are the key factors of development the adequate structures and mechanisms within the state machine. Matania, Yoffe and Goldstein (Matania et al. 2017) outline the necessity in the next phase of evolution of governmental structures – the formation of a single civilian entity with concrete operational capabilities, responsible for defending the national cyberspace and leading national cybersecurity efforts [2].

3 Hypothesis

Singapore is a first jurisdiction in South-East region that has developed its cybersecurity legislation to impose requirements on certain businesses to implement protections against cybersecurity risks into their computer systems. Taking into account its leading role in regional and international economic relations and digitalization processes the CSA clauses should be thoroughly considered and positive experience in regulation of the mentioned sphere applied.

4 Results and Discussion

The internationally recognized definition of the critical information infrastructure is very broad, such as European Commission in its Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection considers information and communication technologies systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.) [7]. In the Green Paper on a European Programme for Critical Infrastructure Protection [8] the European Commission provides an indicative list of 11 critical sectors: Energy, Information, Communication Technologies (ICT), Water, Food, Health, Financial, Public & Legal Order and Safety, Civil Administration, Transport, Chemical and Nuclear Industry, Space and Research.

Therefore every state sets the criteria for the declaration of any data, database, network, communications infrastructure, (or part thereof), or anything associated with them as the CII. National authorities have to identify the CII and in this process of identification they have launched different initiatives regarding this topic while others are starting now to develop their own approaches [9]. That leads to the difference in the national mechanisms of CII protection depending on the information assets, authorities' powers, methods of regulation, etc. Within the EU Member States have highlighted their own list of critical sectors based on the special characteristics and peculiarities of each country, adding with some new: e.g. Austria excluded Chemical and Nuclear Industry, France excluded Chemical and Nuclear Industry but included Industry; Italy and Greece excluded almost all sectors except Energy and Transport; UK excluded Public & Legal Order, Chemical and Nuclear Industry, Space and Research but included Emergency services [9].

Analysts observe four different maturity levels with regards to CII activities across the states. Level 1 is being characterized with the absence of activities related to the protection of CII; states have identified only transport and energy as critical sectors. At maturity level 2 the state identifies the information and communications technology sector as one of critical sectors that should be addressed. At the level 3 states develop a general methodological framework for the identification of critical information assets with specific steps and responsibilities assigned to involved stakeholders. And the highest maturity level 4 outlines the development of a definition for CII and establishment of specific criteria for the identification of CII assets. At this level states are being considered as the mostly advanced in the area of the CII protection and have taken specific measures for the identification and protection of CII assets [9].

The crucial factor for the CII protection is the effective collaboration between public sector (Government & mandated Agencies) and the private sector, which often controls numerous critical infrastructures. It is a common practice that the service providers are defined by the mandated agency as operators of CIIs: they offer certain critical services to public, support the large scope of the population and the territory, their risks may become the national ones. They are responsible for determining the core processes, the respective applications and, as a last step, the network assets and services (connectivity solutions) which are used to operate the respective applications. An asset can be critical related to (a) the business value, (b) the scope of the population served or (c) the technical dependence of critical applications and this classification depends on the sector and the role of the CII [9].

There are two different approaches for an identification of critical services depending on the leading role for such identification. The state-driven approach assumes the leading role of the government agencies that have the mandate to identify and protect CII and the operator-driven approach assumes the leading role of the CII operators. The latter is performed in France, where the state identifies a list of operators (called also 'vital operators'), who are responsible to identify the individual critical services and assets that comply with a number of risk analyses and risk management directives. Then, the responsible ministries review the selected services and assets along with the drafted CII protection plans. This is a pragmatic approach given the current state of the art of CII identification since operators have a better knowledge of

their infrastructures. It also represents a shift of the effort needed to the operator to which is delegated the accountability [9].

The essence of standards for the CII protection implemented by the CSA in Singapore emphasizes cybersecurity as a default consideration, which means that developers of Smart City eco-systems will need to provide the reassurance and security required within interconnected networks and devices in order for such eco-systems to flourish. The Singapore's emphasis of protecting CII mirrors the position taken in other countries and regions, notably in European Union and in China, emphasizing the need for parties who are interconnected within the eco-system in which CII owners and operators operate to adopt a harmonized approach [10].

Singapore's Cybersecurity Strategy distinguishes four core pillars. The first one is to strengthen the resilience of CIIs by mobilizing businesses and the community. The second pillar is the safety of cyberspace, where all cyber threats are countered; cybercrime is combated and personal data are protected. The third pillar is a developed vibrant cybersecurity ecosystem comprising a skilled workforce, technologically-advanced companies and strong research collaborations, so that it can support Singapore's cybersecurity needs and be a source of new economic growth. And the last but not the least pillar is the forging of strong international partnerships [11].

In 2016 Singapore has identified a list of CII sectors which are services (government and emergency services, healthcare, media, and banking and financial services), utilities (power, water and telecommunications), and transport (land transport, maritime and port, civil aviation) [11]. In 2018 the CSA scoped the CII sectors within a term "essential service", which means any service essential to the national security, defense, foreign relations, economy, public health, public safety or public order of Singapore, and specified them in the First Schedule (46 in a list): services relating to energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, media, and services relating to functioning of Government [12].

The CSA defines "critical information infrastructure" as a computer or a computer system that is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and is located wholly or partly in Singapore (section 2, section 7(1)).

The designed framework for the CII protection is being headed by Commissioner of Cybersecurity (Commissioner). Deputy Commissioner and one or more Assistant Commissioners of Cybersecurity assist the Commissioner in the discharge of the Commissioner's duties and functions (section 4). Duties and functions of Commissioner are stated in a Clause 5 of the CSA. They comprise among many others such duties as identification and designation of CII, regulation of owners of CII with regard to the cybersecurity of the CII (section 5(e)); establishment of cybersecurity codes of practice and standards of performance for implementation by owners of CII (section 5 (f)); licensing and establishment of standards in relation to cybersecurity service providers (section 5(j)); establishment of standards within Singapore in relation to cybersecurity products or services, and the recommended level of cybersecurity of computer hardware or software, including certification or accreditation schemes (section 5(k)).

The most sufficient parts of the CSA are parts 3, 4 and 5. Part 3 provides for the designation of CII and the regulation of owners of CII with regard to the cybersecurity of the CII. Part 4 provides for the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore. Part 5 provides for the licensing of providers of licensable cybersecurity services. The Commissioner of Cybersecurity office is responsible for implementing the provisions of above-mentioned parts.

As for the designation of CII the Commissioner may, by written notice to the owner of a computer or computer system, designate the computer or computer system as a CII. To ascertain if computer or computer system fulfils criteria of CII the Commissioner has a power to obtain the necessary information from the owner of such computer or computer system and to require the owner of a CII to furnish information relating to CII. The CSA grants a right to withhold such information in a case it is protected by law, contract, or the rules of professional conduct (section 8(5)). However, a contractual obligation remains an invalid excuse for refusing to disclose information in the context of (i) an information request pertaining to a known CII or (ii) investigations of cybersecurity incidents (section 19(6)). Under the CSA, the CII owner will not be treated as being in breach of any such contractual obligation if the disclosure was done with reasonable care and in good faith for the purpose of complying with such an information request. However, these provisions still risk raising concerns with businesses about protection of their commercially sensitive information. The CSA requires owners of CII to report "prescribed" cybersecurity incidents or any other incidents specified by the Commissioner. Previously, the Draft Bill required the reporting of all "significant" cybersecurity incidents. Prescribed cybersecurity incidents requiring notification will be set by the Commissioner [13].

The Commissioner is also empowered to issue written directions which may relate to (a) the action to be taken by the owner or owners in relation to a cybersecurity threat; (b) compliance with any code of practice or standard of performance applicable to the owner; (c) the appointment of an auditor approved by the Commissioner to audit the owner or owners on their compliance with this Act or any code of practice or standard of performance applicable to the owner or owners; (d) such other matters as the Commissioner may consider necessary or expedient to ensure the cybersecurity of the critical information infrastructure (section 12).

The CSA requires audits at least once every two years and risk assessments once a year for the affirmation of compliance of the CII with this Act and the applicable codes of practice and standards of performance, to be carried out by an auditor approved or appointed by the Commissioner (section 15). Clause 15 implies severe consequences in a case of violation of this provision – the owner of the CII shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

The prevention of cybersecurity incidents is fulfilled by conducting compulsory cybersecurity exercises for the purpose of testing the state of readiness of owners of different CII in responding to significant cybersecurity incidents. The Commissioner writes a direction and any person who, without reasonable excuse, fails to comply it

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 (section 16).

On respond to cybersecurity threats and incidents the Commissioner empowered to investigate and prevent cybersecurity incidents including the serious ones by (1) receiving signed statements, physical or electronic records and documents; (2) examining orally any person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or incident; (3) appointing cybersecurity technical experts etc. (sections 19, 20, 22).

Clause 23 empowers the Minister to authorize or direct any person or organization to take emergency cybersecurity measures and comply with necessary requirements, for the purposes of preventing, detecting or countering any serious and imminent threat to the CII. Those measures or requirements (a) do not confer any right to the production of, or of access to, information subject to legal privilege; and (b) have effect despite any obligation or limitation imposed or right, privilege or immunity conferred by or under any law, contract or rules of professional conduct, including any restriction on the disclosure of information imposed by law, contract or rules of professional conduct. The CSA obliges any person to meet the requirements of the specified person otherwise he or she shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both. Clause 23 comprises detailed specifications on different aspects of meeting the emergency measures and requirements.

Another specific feature of the CSA that makes it a new generation standard is a licensing framework for cybersecurity service providers. It is aimed to assure a safety and security to consumers of cybersecurity services, to address information asymmetry in the industry and to provide the improvement of the standards of cybersecurity service providers and professionals. Section 24 details the main principle of the CSA - no person to provide licensable cybersecurity service without license. Licensing functions are assigned to the Commissioner who is responsible for the administration of that framework. The licensable cybersecurity services are (a) managed security operations centre (SOC) monitoring service; and (b) penetration testing service.

Managed security operations centre (SOC) monitoring service is a service for the monitoring of the level of cybersecurity of a computer or computer system of another person by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system.

Penetration testing service is a service for assessing, testing or evaluating the level of cybersecurity of a computer or computer system, by searching for vulnerabilities in, and compromising, the cybersecurity defenses of the computer or computer system, and includes any of the following activities: (a) determining the cybersecurity vulnerabilities of a computer or computer system, and demonstrating how such vulnerabilities may be exploited and taken advantage of; (b) determining or testing the organization's ability to identify and respond to cybersecurity incidents through simulation of attempts to penetrate the cybersecurity defenses of the computer or computer system; (c) identifying and quantifying the cybersecurity vulnerabilities of a computer or computer system, indicating vulnerabilities and providing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an

acceptable level of risk; (d) utilizing social engineering to assess the level of vulnerability of an organization to cybersecurity threats (Second Schedule).

The CSA envisages three types of licenses depending on their conditions specified: (a) general (conditions are applicable to all licensees); (b) specific (conditions are applicable to a specified class of licensees); and (c) individual (conditions are applicable to a specified licensee only). A license is in force for such period (not exceeding 5 years) as the licensing officer may specify in the license, starting from the date of its issue. Such a discretionary authority of the Commissioner provides for the optimal protection of the CII. A licensee is obliged to fulfill the requirements imposed by the CSA (first of all it's a duty to keep records of the information necessary for the CII protection for three years) and is a subject of financial penalty if fails to comply with it (a fine not exceeding $10,000 or imprisonment for a term not exceeding 12 months or both).

The appeal authority in a licensing framework is a Minister and the Clause 35 provides for an avenue of appeal to the Minister against decisions made by the licensing officer. The decision of the Minister on an appeal is final (section 35(7)).

5 Conclusions

Singapore implements the state-driven approach for the CII protection. At the same time this approach is well-balanced and calibrated. The legislature has tried to harmonize the efficient powers of authorities with the burdens imposed on companies and private individuals in the IT industry. The CSA establishes a solid and precise framework for the CII protection specifying three core aspects: (1) constant cooperation of public authorities and private sector in envisaging the CII system; (2) broad authorities for prevention, management and response to cybersecurity threats and incidents in Singapore, and (3) compulsory licensing of cybersecurity services. It emphasizes on compliance with promulgated codes of practice and expresses designation of CII and cybersecurity threats. The distinctive feature of the CSA is its significant reduction of the compliance burden on cybersecurity professionals and CII owners. As for the CII protection it's important that computer systems in the supply chain supporting the operation of a CII (i.e. data centre owners and cloud services operators) will not be designated as CIIs. Thus the CSA illustrates the narrow approach of law makers in envisaging the CSA jurisdiction – it implies just CII owners and not any network operators. At the same time the CSA has created some temporary uncertainties, for example, it contains a term "debilitating effect" (section 7(1)) referring to availability of an essential service. It is expected to be fixed in the upcoming Cybersecurity Act's Regulations containing detailed prescriptions relating to the practical operation of the CSA: the process for the designation of CII, the standards to be maintained by an owner of CII, the responsibilities and duties of an owner of a CII and the type of changes that are considered material changes to the design, configuration, security or operations of CII to be reported by an owner of CII [13, 14]. All above-mentioned characterizes the CSA as a new generation standard for the CII protection in a modern high-risk digital world.

References

1. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S.: Catastrophic cascade of failures in interdependent networks. Nature **464**(7291), 1025–1028 (2010)
2. Matania, E., Yoffe, L., Goldstein, T.: Structuring the national cyber defence: in evolution towards a Central Cyber Authority. J. Cyber Policy **2**(1), 16–25 (2017)
3. Farrand, B., Carrapico, H.: Blurring public and private: cybersecurity in the age of regulatory capitalism. In: Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance, pp. 197–217. Springer International Publishing AG, Basel (2018)
4. Sarri, A., Moulinos, K.: Stocktaking, Analysis and Recommendations on the Protection of CIIs. European Union Agency for Network and Information Security (ENISA), Heraklion (2015)
5. Häyhtiö, M., Zaerens, K.: A comprehensive assessment model for critical infrastructure protection. Manag. Prod. Eng. Rev. **8**(4), 42–53 (2017)
6. Bobro, D.: Methodological aspects of critical infrastructure protection (2018). Research Gate Homepage. https://www.researchgate.net/publication/322715607_The_National_Institute_for_Strategic_Studies_methodological_aspects_of_critical_infrastructure_protection. Accessed 21 May 2018
7. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. Official J. L, **345**(23), 12 (2008)
8. Green Paper on a European Programme for Critical Infrastructure Protection. COM 576 final (2005)
9. Mattioli, R., Levy-Bencheton, C.: Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks. European Union Agency for Network and Information Security (ENISA), Heraklion (2014)
10. Wun, R., Tan, M.: Cybersecurity in Singapore and China (2018). Lexology Homepage. https://www.lexology.com/library/detail.aspx?g=cae1ecf3-8228-4f89-a30e-6587fd592da4. Accessed 21 May 2018
11. Singapore's Cybersecurity Strategy. Cyber Security Agency of Singapore, Singapore (2016)
12. Cybersecurity Act: Cyber Security Agency of Singapore, Singapore (2018)
13. Singapore's New Cybersecurity Act - A Relief and Leading the Way for Others? BakerMcKenzie Homepage. https://www.bakermckenzie.com/en/insight/publications/2018/02/singapores-new-cybersecurity-act. Accessed 21 May 2018
14. Hashim, H.M., Sokolova, E., Derevianko, O., Solovev, D.B.: Cooling load calculations. In: IOP Conference Series: Materials Science and Engineering, vol. 463, Part 2, Paper № 032030 (2018). https://doi.org/10.1088/1757-899X/463/3/032030