TECHNICAL COMPENDIUM

SUPPLY CHAIN SECURITY IN THE CYBER AGE

SECTOR TRENDS, CURRENT THREATS AND MULTI-STAKEHOLDER RESPONSES

OLEG DEMIDOV & GIACOMO PERSI PAOLI

40 UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

UNIDIR's Security and Technology Programme is supported by the Governments of Germany, the Netherlands, Norway and Switzerland. The authors would like to thank Mr. Chris Nissen, Director, Asymmetric Threat Response and Supply Chain Security at The MITRE Corporation; Mr. Donald A. (Andy) Purdy, Jr., Chief Security Officer at Huawei Technologies (United States of America); Mr. Kai Michael Hermsen, Global Coordinator for the Charter of Trust at Siemens AG; and Ms. Kerstin Vignard, Head of the support team to General Assembly processes pursuant to resolutions 73/27 and 73/266 at UNIDIR for discussing the report's content and providing feedback and recommendations.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

www.unidir.org

TABLE OF CONTENTS

ABOUT THE AUTHORS

OLEG DEMIDOV is a Cyber Researcher with the Security and Technology Programme at UNIDIR. He graduated from Moscow State University of Lomonosov. Since 2011, he has been conducting research on cybersecurity policy, cyber governance and global Internet governance, critical information infrastructure protection, and international security implications of emerging technologies. Prior to joining UNIDIR, Oleg led the International Cyber Security and Global Internet Governance Program at the non-governmental think tank PIR Center.

GIACOMO PERSI PAOLI is the Programme Lead for Security and Technology at UNIDIR. His expertise spans the science and technology domain, with emphasis on the implications of emerging technologies for security and defence. Prior to joining UNIDIR, he was Associate Director at RAND Europe, where he led the national security, resilience and cyber portfolio, with recent work on cyber acquisition, cyber policy and strategy, and cyber capability development.

ABBREVIATIONS AND ACRONYMS

AIA	Aerospace Industries Association
app	application
BES	Bulk Electric System
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CMMC	Cybersecurity Maturity Model Certification
CNSS	Committee on National Security Systems
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
G7	Group of Seven
G8	Group of Eight
GTI	Global Transparency Initiative
HCSEC	Huawei Cyber Security Evaluation Centre
ICT	information and communications technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGO	intergovernmental organization
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	information technology
MAC	media access control
NATF	North American Transmission Forum
NCSC	National Cyber Security Centre
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OHSAS	Occupational Health and Safety Assessment Series
O-TTPS	Open Trusted Technology Provider Standard
R&D	Research and Development

SAFECode	Software Assurance Forum for Excellence in Code
SCRM	Supply Chain Risk Management
SOC	Service Organization Control
TAPA	Transport Asset Protection Association
TC	Transparency Center
TCSEC	Trusted Computer System Evaluation Criteria

ABSTRACT

This publication is a technical compendium to UNIDIR's report *Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses*. The compendium is supplementary to the report and provides more detailed information and case-based analysis related to the report's major sections in a number of annexes.

In particular, the compendium includes (i) an overview of standardized definitions of key terms related to information and communications technology (ICT) supply chain security and integrity, (ii) highlights from selected cases of supply chain cyberattacks, and (iii) an overview and mapping of major standardization frameworks aimed at strengthening security and integrity in ICT supply chains. The compendium also provides a detailed analysis of government and industry-led guidelines and best practices for cyber supply chain risk management (SCRM), examples of corporate supply chain assurance frameworks from the technology sector, and self-assessment and auditing tools for cyber SCRM. Finally, the publication maps and provides details on international and multi-stakeholder norm-developing initiatives addressing supply chain security and integrity.

The technical compendium's primary target audience might include private industry and technology sector experts, as well as security policy researchers interested in a more case-based and technology-specific elaboration of the technology supply chain security and integrity issues covered in UNIDIR's report. However, the compendium aims to be useful to all audiences targeted by the report, including diplomats, representatives of intergovernmental organizations and policymakers.

ANNEX I

Standardized definitions of key terms related to the security and integrity of information and communications technology supply chains

Table I.1. Standardized definitions of key terms related to the security and integrity of information and communications technology supply chains

NO.	TERM	DEFINITION	ORGANIZATION (TYPE)	SOURCE
1.	Supply chain	"The system of organizations, people, activities, information, and resources involved from development to delivery of a product or service from a supplier to a customer. Supply chain 'activities' or 'operations' involve the transformation of raw materials, components, and intellectual property into a product to be delivered to the end customer and necessary coordination and collaboration with suppliers, intermediaries, and third-party service providers."	The MITRE Corporation *(private sector / technology community)*	Deliver Uncompromised – A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War[1]
2.		"Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer."	US National Institute of Standards and Technology (NIST) *(government)*	NIST Special Publication 800-53, Rev. 4. (ISO 28001:2007 – adapted)[2]
3.		"The network of retailers, distributors, transporters, storage facilities, and suppliers that participate in the sale, delivery, and production of a particular product."	US National Institute of Standards and Technology *(government)*	NIST Special Publication 800-98[3]

NO.	TERM	DEFINITION	ORGANIZATION (TYPE)	SOURCE
4.		"Set of organizations with linked set of resources and processes, each of which acts as an acquirer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement "Note 1...: A supply chain can include vendors, manufacturing facilities, logistics providers, distribution centres, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, and handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services. "Note 2...: The supply chain view is relative to the position of the acquirer."	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) *(intergovernmental organizations [IGOs])*	ISO/IEC 27036-1:2014[4]
5.		"A system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier (producer) to customer"	European Union Agency for Network and Information Security *(government / IGO)*	Supply Chain Integrity – An Overview of the ICT Supply Chain Risks and Challenges, and Vision for the Way Forward[5]
6.		"In general refers to the whole life of an IT product or service in an organisation. It likely includes multiple organisations. Supply chain includes the linked processes of design, manufacture, supply, delivery, support and decommissioning of equipment (hardware and software) or services that are utilised within an organisation's cyber ecosystem"	Australian Cyber Security Centre *(government / technology community)*	Cyber Supply Chain Risk Management – Practitioners Guide[6]

NO.	TERM	DEFINITION	ORGANIZATION (TYPE)	SOURCE
7.		A set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to customers.	Open Trusted Technology Forum[7] *(private sector / technology community)*	Open Trusted Technology Provider Standard (O-TTPS)[8]
8.	ICT/cyber/ technology supply chain	Information and communications technology (ICT) supply chain: "Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer."	US National Institute of Standards and Technology *(government)*	Special Publication 800-161[9]
9.		Cyber supply chain: "includes the design, manufacture, delivery, deployment, support and decommissioning of equipment (hardware and software) or services that are utilised within an organisation's cyber ecosystem. Supply chain must consider the whole life of an [information technology (IT)] product or service in an organisation."	Australian Cyber Security Centre *(government / technology community)*	Cyber Supply Chain Risk Management – Practitioners Guide
10.		Technology supply chain: The manufacturing and/or development process used to produce and deliver hardware or software technology products and their configuration.	Open Trusted Technology Forum *(private sector / technology community)*	Open Trusted Technology Provider Standard (O-TTPS)
11.	Supply chain integrity	"Indication of the conformance of the supply chain to good practices and specifications associated with its operations"	European Union Agency for Network and Information Security *(government / IGO)*	Supply Chain Integrity – An Overview of the ICT Supply Chain Risks and Challenges, and Vision for the Way Forward

NO.	TERM	DEFINITION	ORGANIZATION (TYPE)	SOURCE
12.	Supply chain security	"Security of the processes, techniques, and technologies associated with supply chains"	European Union Agency for Network and Information Security *(government / IGO)*	Supply Chain Integrity – An Overview of the ICT Supply Chain Risks and Challenges, and Vision for the Way Forward
13.		The manufacturing and/or development process performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation. Extends the US NIST definition [NIST 800-12].	Open Trusted Technology Forum *(private sector / technology community)*	Open Trusted Technology Provider Standard (O-TTPS)
14.	Supply chain attack	"Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle."	Committee on National Security Systems *(government)*	Committee on National Security Systems (CNSS) Glossary[10]
15.		An attempt to disrupt the creation of goods by subverting the hardware, software, or configuration of a commercial product, prior to customer delivery (e.g., manufacturing, ordering, or distribution) for the purpose of introducing an exploitable vulnerability.	Open Trusted Technology Forum *(private sector / technology community)*	Open Trusted Technology Provider Standard (O-TTPS)
16.		"An intentional malicious action (e.g., insertion, substitution or modification) taken to create and ultimately exploit a vulnerability in Information and Communication Technology (hardware, software, firmware) at any point within the supply chain with the primary goal of disrupting or surveilling a mission using cyber resources."	The MITRE Corporation *(private sector / technology community)*	Supply Chain Attacks and Resiliency Mitigations – Guidance for System Security Engineers[11]

NO.	TERM	DEFINITION	ORGANIZATION (TYPE)	SOURCE
17.	Supply chain risk	"Refers to the combination of vulnerabilities in an organisation's supply chain, the threats that organisation's supply chain is likely exposed to, and the impact of a realised vulnerability by a threat."	Australian Cyber Security Centre *(government / technology community)*	Cyber Supply Chain Risk Management – Practitioners Guide
18.		"Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation."	US National Institute of Standards and Technology *(government)*	NIST Special Publication 800-161
19.	ICT supply chain compromise	"An occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service."	US National Institute of Standards and Technology *(government)*	NIST Special Publication 800-161
20.	Supply chain risk managemen t	"The implementation of processes, tools or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle."	US National Institute of Standards and Technology *(government)*	NISTIR 8074, Vol. 2[12]
21.		"Refers to the process of identifying supply chain threats and vulnerabilities to determine the most likely risks, and ultimately the treatment of high supply chain risks."	Australian Cyber Security Centre *(government / technology community)*	Cyber Supply Chain Risk Management –Practitioners Guide

NO.	TERM	DEFINITION	ORGANIZATION (TYPE)	SOURCE
22.		The identification, assessment, prioritization, and mitigation of business, technical, and physical risks as they pertain to the manufacturing process including the use of third-party components and services in addition to the delivery of the product to the end user.	Open Trusted Technology Forum *(private sector / technology community)*	Open Trusted Technology Provider Standard (O-TTPS)
23.	ICT supply chain risk managemen t	"The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains."	US National Institute of Standards and Technology *(government)*	Special Publication 800-161
24.	Supplier	"Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products [or] services provided to that organization's Buyers."	US National Institute of Standards and Technology *(government)*	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1[13]
25.		"Organization or an individual that enters into agreement with the acquirer for the supply of a product or service"	International Organization for Standardization / International Electrotechnical Commission *(IGOs)*	ISO/IEC 27036-1:2014
26.	Vendor	"May include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."	North American Electric Reliability Corporation *(private sector / technology community)*	CIP-013-1 – Cyber Security – Supply Chain Risk Management[14]
27.		"Typically the organisation that supplies a product or service to the customer."	Australian Cyber Security Centre *(government / technology community)*	Cyber Supply Chain Risk Management – Practitioners Guide

NO.	TERM	DEFINITION	ORGANIZATION (TYPE)	SOURCE
28.		"A commercial supplier of software or hardware."	US National Institute of Standards and Technology *(government)*	NISTIR 4734[15]
29.		Builds products or components (hardware or software).	Open Trusted Technology Forum *(private sector / technology community)*	Open Trusted Technology Provider Standard (O-TTPS)

ANNEX II

Examples of supply chain attacks

Table II.1. Examples of supply chain attacks

NO.	ATTACK NAME	TIMING	SUMMARY OF THE INCIDENT
1.	Floxif / CCleaner[16]	2017	The incident took place when the download servers used by software vendor Avast to distribute its legitimate software package – a popular operating system maintenance utility, CCleaner 5.33 – were leveraged to deliver malware to multiple users and organizations. A multistage malware payload (backdoor) was inserted in the legitimate signed version of CCleaner 5.33; this malicious code covertly rode on top of the installation of the utility. The attack affected victims – mostly end users – on a massive scale owing to the popularity of CCleaner software. By November 2016, the utility had hit 2 billion downloads (total), with a growth rate of 5 million additional users per week. According to existing estimations, the malicious payload, named Floxif, infected 2.2 million CCleaner customers worldwide. In addition to infecting users' devices en masse, the attackers also targeted 18 companies and infected 40 devices in an espionage effort aimed at gaining access to global microelectronics vendors (Asus, Fujitsu, Intel, O2, Samsung, Singtel, Sony, VMWare and others).

NO.	ATTACK NAME	TIMING	SUMMARY OF THE INCIDENT
2.	NotPetya / MeDoc[17,18]	June 2017	One of the most prominent and massive recent attacks on software supply chains is the Nyetya (Cisco TALOS naming convention) or NotPetya (widely known name) ransomware, which broke out in June 2017. The ransomware did not gain access via an email or document. Instead, its entry point was via the update system for a Ukrainian tax accounting package (MeDoc). Once entry was gained, the adversary analysed the network components, stole credentials and moved laterally, eventually encrypting large amounts of information. Using a variant of a ransomware called Petya, the malware was propagated through two critical vulnerability exploits: the same EternalBlue exploit used in the WannaCry attack, which was combined with a credential-stealing exploit called Mimikatz, created as a proof of concept to demonstrate password-related flaws in Windows systems. NotPetya could be used to pull passwords out of RAM and use them to hack into other machines – including multi-user networks – that could be accessed with the same credentials. This gave attackers the ability to "infiltrate a target, exfiltrate massive amounts of data, encrypt the original data and hold the stolen data for a bigger ransom". NotPetya effectively improved on the original Petya ransomware's capability of encrypting the master boot record by also encrypting the master file table and deleting the key. This, in effect, rendered the ransomware a "wiper" and allowed it to overwrite and ultimately wipe the affected system's hard disk. By targeting legitimate Ukrainian accounting software as the point of entry, the malicious tool spread laterally across corporate networks to deploy its payload, with crippling damage to companies across the globe: its reported cost to US FedEx and to global naval shipping operator Maersk was estimated at $3 million each.

NO.	ATTACK NAME	TIMING	SUMMARY OF THE INCIDENT
3.	Operation ShadowHammer	June–November 2018	This sophisticated information and communications technology (ICT) supply chain attack was discovered in a few months by Kaspersky.[19] The attack involved Asus Live Update, a utility that is pre-installed on most Asus computers and is used to automatically update certain components, such as the BIOS, the UEFI, drivers and applications (apps). According to Kaspersky, the attackers targeted an unknown pool of users, who were identified by their network adapters' media access control (MAC) addresses. The attack path compromised servers used for the Asus Live Update tool and inserted a malicious payload. The malicious file was signed with legitimate Asus digital certificates, thus appearing to users' devices and their security software to be authentic software from the vendor. According to the estimates, the attack continued for 5 months, leading to over 500,000 users downloading infected updates from the Asus server. Almost 50% of the backdoor downloads were made by users from France, Germany and the Russian Federation, with users from a dozen other states also affected. Despite these figures, security researchers believe that the attack was aimed at a particular group of users or organizations, as after installation on a device, the malware searched for targeted systems through their unique MAC addresses, in total about 600 of them. This made security researchers believe that the attack was a tailored operation with level of sophistication potentially exceeding Floxif/CCleaner and some other prominent cases of software supply chain attacks.

NO.	ATTACK NAME	TIMING	SUMMARY OF THE INCIDENT
4.	Cryptominer attack on PDF editor app (unnamed)	July 2018 *(reported)*	An unusual case of a "multi-tier" software supply chain attack involving Microsoft's Windows Defender Advanced Threat Protection.[20] According to Microsoft, attackers compromised the shared digital infrastructure in place between an unnamed vendor of a PDF editor app and one of its software vendor partners. As a result, the PDF editor app's legitimate installer was turned into a carrier of a malicious payload, similar to the mechanics of the CCleaner 5.33 attack. This case is considered unusual and sophisticated, as the first vendor's systems were not affected by the malware. The entry point of the payload was traced to a second software vendor, which hosted additional packages used by the PDF editor app during installation (the second-tier supply chain). Unlike previously described cases, this attack was not targeted at particular organisations or end users: the attackers took advantage of their campaign by installing cryptocurrency miners on infected systems. Also, the scale of infection turned out to be quite limited. However, the attack highlighted some new patterns, such as the escalating frequency of software supply chain attacks and the increasing use of cryptocurrency miners as primary means for monetizing malware campaigns. The attack in a certain way mirrors the mounting complexity of digital supply chains by bringing the multi-tier approach common in ICT supply chain and vendor relations to the cyberattack domain.

ANNEX III

Standardization frameworks addressing the security and integrity of information and communications technology supply chains

Table III.1. Standardization frameworks addressing the security and integrity of information and communications technology supply chains

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
RISK ASSESSMENT AND RISK MANAGEMENT STANDARDS				
1.	ISO/IEC 16085:2006. Systems and Software Engineering – Life Cycle Processes – Risk Management[21]	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) *(international standardization bodies)*	2006 *(adopted)* 2017 *(last reviewed and confirmed)*	ISO/IEC 16085 defines a process for the management of risk in the life cycle of software and systems. The standard can be added to the existing set of system and software life cycle processes defined by ISO/IEC 15288 and ISO/IEC 12207, or it can be used independently. The standard aims to be a critical tool for determining the feasibility of project plans, for improving the search for and identification of potential problems that can affect life cycle activities and the quality and performance of products, and for improving the active management of projects. The standard covers best practices for risk management applicable both to software and to systems (hardware). It does not identify supply chain risk management (SCRM) as a separate category and does not provide specific best practices on this matter. However, the best practices and risk management methodology provided in the standard is in general applicable to SCRM.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
2.	ISO/IEC 27005:2018. Information Technology – Security Techniques – Information Security Risk Management[22]	International Organization for Standardization / International Electrotechnical Commission (*international standardization bodies*)	2018 *(3rd edition adopted and published)*	The standard "provides guidelines for information security risk management" and "supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach". As it is focused on information risk management, ISO/IEC 27005 is discussed separately from the rest of ISO/IEC 27000 family of standards in this annex. The standard does not specify, recommend or name any specific risk management methods to be applied in the information risk management context. Instead, it describes and implies a continual process consisting of a structured sequence of activities, some of which are iterative:[23] • Establish the risk management context (e.g. the scope; compliance obligations; the approaches or methods to be used; and relevant policies and criteria, such as the organization's risk tolerance or appetite). • Quantitatively or qualitatively assess (i.e. identify, analyse, evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a "level of risk". • Treat (i.e. modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those levels of risk to prioritize them. • Keep stakeholders informed throughout the process. • Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
3.	ISO 28000:2007. Specification for Security Management Systems for the Supply Chain[24] ISO 28001:2007 Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments and Plans – Requirements and Guidance[25]	International Organization for Standardization *(international standardization body)*	2014 *(reviewed and confirmed)*	ISO 28000, initially adopted in 2007, specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Thus, the standard was among the first international standardization frameworks to focus on and provide specific guidelines and best practices on supply chain security. In general, ISO 28000:2007 regards security management as being linked to many other aspects of business management, including all activities controlled or influenced by organizations that impact supply chain security. These other aspects should be considered directly when they have an impact on security management, including transporting goods along the supply chain. ISO 28000:2007, as intended, has been quite widely used by organizations running production or supply chain processes to establish, implement, maintain and improve a security management system; assure conformance with stated security management policy; seek certification or registration of security management systems by an accredited third-party certification body; or make a self-determination and self-declaration of conformance with the standard. ISO 28001:2007, elaborating on the provisions of the "parent" standard, provides requirements and guidance for organizations in international supply chains to • Develop and implement supply chain security plans and processes • Establish and document a minimum level of security within a supply chain or segment of a supply chain • Define the portion of an international supply chain within which they have established security

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
				• Conduct security assessments on that portion of the supply chain and develop adequate countermeasures • Train security personnel in their security-related duties As compliance with the standards has become quite a widespread requirement (or market advantage), some of their requirements addressing supply chain security have been included in national legislative and regulatory codes.
4.	ISO 31000:2018. Risk Management – Guidelines[26]	International Organization for Standardization *(international standardization body)*	2018	ISO 31000 provides principles, a framework and a process for managing risk. It can be used by any organization, regardless of its size, activity or sector. The standard aims to help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment. The standard is neither specific to supply chain security and integrity risks nor focused on the information and communications technology (ICT) sector in particular. Also, ISO 31000 cannot be used for certification purposes, as it provides only generic guidelines related to risk management in organizations. However, the standard still should be considered within the context of ICT supply chain security and integrity as it provides a fundamental methodological basis for organizations of any size and in any sector, including ICT or technology, to assess and manage risks. One of the critical areas of risk management addressed by the standard is internal and external audit programmes, which are also essential for assessing and managing supply chain security and integrity risks, as well as risks associated with ICT products and systems developed, used or procured by organizations throughout their life cycles.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
INFORMATION SECURITY STANDARDS				
5.	ISO/IEC 15408. Product Security (through Common Criteria for Information Technology Security Evaluation)[27]	International Organization for Standardization / International Electrotechnical Commission *(international standardization bodies)*	2015 *(last reviewed and approved)*	An international computer security certification standard adopted and approved by ISO on the basis of the Common Criteria for Information Technology Security Evaluation (Common Criteria or CC). The CC are not a single standard specification, but an international information technology (IT) security evaluation methodological framework. The CC were developed to define and facilitate consistent evaluations of security products and systems and to enable certification of IT products against standard specifications ("Protection Profiles") representing the baseline set of security requirements for computer systems and products. Historically, the CC emerged out of three IT security standards: • Information Technology Security Evaluation Criteria: The European standard, developed in 1991 jointly by France, Germany, the Netherlands and the United Kingdom • Trusted Computer System Evaluation Criteria (TCSEC): A standard initially developed in 1983 by the US Department of Defense (DoD) • Canadian Trusted Computer Product Evaluation Criteria: A Canadian standard that followed from the US TCSEC in 1993 and was used jointly in the United States of America and Canada to conduct security evaluations of IT products

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
				As of today, the CC include 14 categories of Protection Profiles, with the total number of such profiles developed by different countries on the basis of the CC methodology being over 190.[28] The CC framework is used and mutually recognized by 30 States[29] on the basis of the Common Criteria Recognition Arrangement (CCRA), signed in 2000. The key aim of the CCRA is to enable IT products that earn a CC national certificate to be procured and used without the need for further evaluation across the markets of other CCRA Member States. As of August 2019, 16 CCRA members have licensed laboratories[30] that conduct CC-based security evaluation and issue CC certificates for IT products and systems. The CC framework is not specific to ICT supply chains and does not specify "supply chain" as a separate object of protection. However, certification for CC provides an important element for testing and providing information assurance in IT products released on the market. The CC testing methodology, in most cases, enables compromises in the supply chains of tested products to be identified; compromised IT products would not pass the CC tests successfully.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
6.	ISO/IEC 27000. Information Technology – Security Techniques[31] (series of standards)	International Organization for Standardization / International Electrotechnical Commission *(international standardization bodies)*	2018 *(last reviewed and confirmed)*	ISO/IEC 27000 is one of the most commonly known "families" of information security standards. The series provides a wide spectrum of best practices and currently includes over 40 standards (from ISO/IEC 27001 to ISO/IEC 27050-1/-2 and ISO 27799). The family of standards provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems. Information security is defined and addressed within the standards family in the context of the confidentiality–availability–integrity triad. Some of the standards in the ISO/IEC 27000 family directly address acquisition and supplier relationships in the information security context (e.g. Chapters 14 and 15 of ISO/IEC 27002 address supply chain-related issues):[32] • Chapter 14, "System acquisition, development and maintenance": Addresses the security requirements of information systems, as well as security in development and support processes and test data • Chapter 15, "Supplier relationships": Addresses information security in supplier relationships and supplier service delivery management In the ISO/IEC 27000 standards series, information security controls and their objectives are specified and outlined. The information security controls are generally regarded as the best practice in achieving those objectives. For each of the controls, the standards provide specific implementation guidance. The family of standards provides a fundamental framework for the information security and cybersecurity of the supply chain. However, it does not identify and address ICT supply chains as a separate niche, nor does it provide in-depth and detailed guidance on sector-specific or niche-specific supply and acquisition information security controls.

7.	ISO/IEC 27036-1:2014. Information Technology – Security Techniques – Information Security for Supplier Relationships[33]	International Organization for Standardization / International Electrotechnical Commission *(international standardization bodies)*	2013 *(adopted)* 2018 *(reviewed and approved)*	This was the first ISO standard with a particular focus on information security and cybersecurity for the ICT supply chain, addressing the perspectives of both acquirers and suppliers. The introductory part of the standard provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of the standard.[34] Part 2 of the standard specifies fundamental cybersecurity requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships. These requirements cover any procurement and supply of products and services, such as manufacturing or assembly, business processes, software and hardware components, knowledge processes, build–operate–transfer, and cloud computing. Thus, the standard fully covers the ICT supply chain niche. Also, the standard's requirements are intended to be applicable to all organizations, regardless of type, size or nature. While the standard covers many supplier relationship security issues that are, in general terms, encompassed by ISO/IEC 27002, its Part 3, "Guidelines for ICT supply chain security", provides additional guidance in the specific context of ICT supplies. The standard guides both suppliers and acquirers of ICT goods and services on (i) information risk management relating to the widely dispersed and complex supply chain, including risks such as malware and counterfeit products, plus "organizational risks", and (ii) the integration of risk management with system and software life cycle processes, drawing on other international standards such as ISO/IEC 15288, 12207 and 27002. One of the things that the standard misses, according to the *Supply Chain Integrity* guide from the European Union Agency for Network and Information Security,[35] is the integrity of ICT supply chains.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
SYSTEMS ENGINEERING STANDARDS				
8.	ISO/IEC/IEEE 12207:2017. Systems and Software Engineering – Software Life Cycle Processes[36]	International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers (IEEE) *(international standardization bodies)*	2017 *(last updated)*	The standard is one of the major international standards for software life cycle processes; it aims to encompass all the processes required to develop and maintain software systems, including the outcomes and activities of each process. Hence, its scope with regard to supply chains is limited to software supply chains and, thus, is narrower than ICT supply chains (e.g. it does not include hardware). In particular, the standard includes the acquisition and supply processes, describing them as activities related to establishing an agreement between a supplier and an acquirer. According to the standard, acquisition covers all the activities involved in initiating a project. The acquisition phase can be divided into different activities and deliverables, which are completed chronologically. Although the standard provides a detailed framework for defining, controlling and improving software life cycle processes within an organization or a project, it does not identify or describe the security and integrity of software supply chains as a separate item for detailed analysis.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
9.	ISO/IEC/IEEE 15288:2015. Systems and Software Engineering – System Life Cycle Processes[37]	International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers *(international standardization bodies)*	2015 *(adopted)*	The standard establishes a common framework of process descriptions for describing the life cycle of manufactured systems. It defines a set of processes and associated terminology from an engineering viewpoint. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of processes can be applied to manage and perform the stages of a system's life cycle. This is accomplished through the involvement of all stakeholders. The standard also provides processes that support the definition, control and improvement of the system life cycle processes used within an organization or a project. Organizations and projects can use these processes when acquiring and supplying systems. The standard concerns systems that may be configured with one or more of the following system elements: hardware, software, data, humans, processes (e.g. processes for providing services to users), procedures (e.g. operator instructions), facilities, materials and naturally occurring entities. Accordingly, supply chains are regarded in the standard through the lens of such elements and their combination. However, the standard does not address supply chain security and integrity specifically, nor does it consider ICT supply chains as a separate and specific category of supply and acquisition system.
PRODUCT AND SERVICE LIFE CYCLE STANDARDS				

10.	Open Trusted Technology Provider Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products[38] (also adopted as ISO/IEC 20243:2015. Information Technology – Open Trusted Technology Provider Standard O-TTPS – Mitigating Maliciously Tainted and Counterfeit Products)[39]	Open Trusted Technology Forum *(industry / technology community)* Also adopted by International Organization for Standardization / International Electrotechnical Commission *(international standardization bodies)*	2014 *(published)* 2015 *(adopted by ISO/IEC)* 2018 *(updated as ISO/IEC 20243-1:2018)*	One of the first standards aimed at ensuring both the integrity of commercial off-the-shelf (COTS) ICT products and the security of their supply chains. The standard focuses on COTS products because such ICT products are procured by both public and private organizations around the world, as well as by end users, and their supply chains are often transnational and cross-border, which further contributes to their being subject to a broader scope of cyber threats and other security risks. The standard is based on and associated with the Open Trusted Technology Provider Framework. Initially released as a white paper in February 2011, the framework serves as a basis for the standard and its further development. The framework is a compendium of organizational guidelines and best practices that, if implemented, enhance the security and integrity of COTS ICT products throughout the entire product life cycle, including its supply chain aspects. The standard defines a set of best practices for COTS ICT providers to mitigate the risk of maliciously tainted and counterfeit components being incorporated into each phase of a product’s life cycle. This encompasses design, sourcing, manufacture, fulfilment, distribution, sustainment and disposal. The best practices apply to in-house development, outsourced development and manufacturing, and global supply chains. The standard has been referred to as a potential benchmark in some national regulatory frameworks. For example, the US National Defense Authorization Act for Fiscal Year 2016 committed the US Secretary of Defense to conduct an assessment of the O-TTPS or similar public, open technology standards and to report to the US Congress.[40] In 2015, the standard was approved and adopted by ISO/IEC as international standard ISO/IEC 20243:2015. In 2018, further development of the standard took place within the ISO/IEC framework, with ISO/IEC 20243-1:2018, Part 1: Requirements and Recommendations published and adopted.[41] The new standard provides a detailed set of guidelines, requirements and

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
				recommendations that address specific threats to the integrity of hardware and software COTS ICT products throughout their product life cycle.[42] The Open Group also developed the O-TTPS Certification Program, serving as a certification scheme that complements the requirements of the O-TTPS. The Open Group certifies organizations that it deems to comply with the programme requirements as Open Trusted Technology Providers. The certification policy (Version 1.1) published in 2017[43] provides detailed workflow diagrams for third-party certification, with additional details for each step of the process. The document also includes specific policies for conformance requirements, certification maintenance and re-certification, as well as an appeal process for certification decisions. The certification programme is one of the first of its kind in providing certification for conforming to standards for product integrity coupled with supply chain security, available to any organization.
SECTOR-SPECIFIC STANDARDS				
11.	NERC CIP-013-1 – Cyber Security – Supply Chain Risk Management[44]	North American Electric Reliability Corporation (NERC) *(industry / private sector)*	August 2017 *(adopted by NERC)* October 2018	The standard was designed and adopted by NERC to proactively mitigate cybersecurity risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for SCRM of BES cyber systems. The standard was developed in response to *Order No. 829, Revised Critical Infrastructure Protection Reliability Standards*, adopted by the US Federal Energy Regulatory Commission, the key federal regulator in the sector of electricity supply and BES, in July 2016.[45] In particular, the order tasked NERC with developing a standard to cover:[46] ○ Software integrity and authenticity ○ Vendor remote access ○ Information system planning

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
			(approved by US Federal Energy Regulatory Commission)	○ Vendor risk management and procurement controls The standard provides a framework of requirements covering different actors (functional entities including grid operators, generator owners and operators, and transmission owners and operators) with different responsibilities and roles in ensuring the reliable operation and cybersecurity of BESs. The requirements for responsible entities provided in the standard are: • Develop documented supply chain cybersecurity risk management plans for high and medium impact cyber systems. • Implement such plans. • Implement periodic review and approval of such plans by a senior critical infrastructure protection manager. The standard also introduces a compliance framework for those requirements, delegating compliance authority to NERC or to US Government agencies. Finally, the standard provides a detailed reference framework for assessing violation severity levels within BESs, with a focus on cyber impacts.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
12.	AS6081. Fraudulent/ Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors[47]	SAE International *(private industry / government)*	2012 *(published)*	SAE International is a US-based, globally active standards-developing organization conducting its activities with a focus on a number of sectors and industries. Historically, its key efforts were made to advance technical standardization in transport industries (e.g. automotive, aerospace, commercial vehicles).[48] This sector-specific standard developed by SAE International addresses the challenge of performance, reliability and safety risks posed by an "increasing and significant volume of fraudulent/counterfeit electronic parts entering the aerospace supply chain".[49] While not being specific to ICT supply chains, the standard encompasses a major share of such chains, covering the niche of electrical, electronic and electromechanical parts (e.g. hardware used in the aerospace industry). The standard provides a framework of best practices to: ○ Identify reliable sources to procure parts ○ Assess and mitigate the risk of distributing fraudulent or counterfeit parts ○ Control suspected and confirmed fraudulent or counterfeit parts ○ Report suspected and confirmed fraudulent or counterfeit parts to other potential users and competent governmental authorities

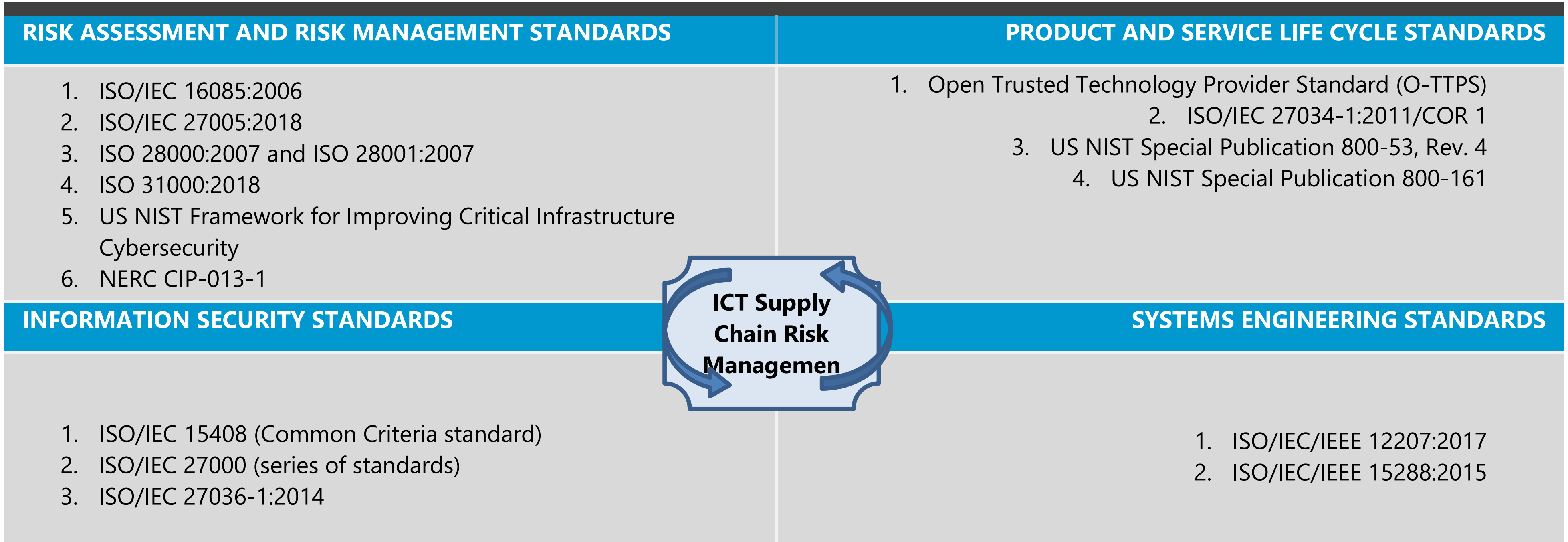
13.	SEMI T20 – Specification for Authentication of Semiconductors and Related Products[50] SEMI T21 – Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain[51]	SEMI *(private industry)*	SEMI T20 – 2015 *(reviewed and approved)* SEMI T21 – 2013 *(approved)*	SEMI is a US-based global industry association of companies that provide equipment, materials and services for the manufacture of semiconductors, photovoltaic panels, LED and flat panel displays, micro-electromechanical systems, printed and flexible electronics, and related micro and nanotechnologies. It was founded in 1970 as an association of semiconductor production equipment vendors. These standards were developed by SEMI as a response to the mounting challenge of contamination of the electronic component supply chain by counterfeit and tainted products. As stressed in SEMI T20, the semiconductor industry has lacked standardized methods to validate the integrity of goods from non-certified distributors or suppliers. The purpose of the specification is to describe the system architecture of an authentication process to establish the trusted identity of products or objects in electronic component supply chains. SEMI T20 encompasses structure, behaviour and services for the organizations and entities involved in authentication of semiconductor and related products or objects throughout their supply chain and manufacturing cycles. Being specific to the semiconductor industry, it does not entirely match the scope of ICT or cyber supply chains. However, owing to the fundamental role of semiconductors and related components in the ICT industry, many of its provisions are potentially applicable to authenticating and ensuring the trustworthiness of ICT supply chain elements. SEMI T20 is the basic element of a suite of SEMI standards aimed at enabling automated, reliable and secure product authentication for the semiconductor industry, thereby reducing the presence of illegal counterfeit items in the marketplace. SEMI T21 is also based on the authentication principles, concepts and best practices summarized in SEMI T20. However, the standard aims to provide best practices for using technical solutions to identify all the buyers of components throughout the supply chain. Thus, SEMI T21 suggests best

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY POINTS
				practices and guidance for using the internationally standardized X.509 digital certificate format to identify buyers in track and trace systems within semiconductor supply chains.
OTHER RELEVANT STANDARDIZATION INITIATIVES				
14.	Considerable developments have been taking place across different frameworks with regard to the security standardization of emerging technologies, including those shaping major segments of technology supply chains or those expected to do so in the years to come. These initiatives include the development of 5G security standards, as well as certification and testing standards for 5G equipment envisioned by the Network Equipment Security Assurance Scheme,[52] a voluntary scheme defined for the mobile industry, developed and defined jointly by two major mobile communications sector standardization bodies: 3GPP and GSMA. These efforts have been closely monitored by some regional actors, such as the European Union: the European Commission identified 5G standards as one of the five priority areas under the Digitising European Industry initiative.[53] While 5G security risks have been one of the aspects covered in the European Union's research publications,[54] in terms of the actual development and adoption of related security standards, the European Union so far has been largely collaborating with the above-mentioned industry associations (3GPP and GSMA) and monitoring their standardization developments.			

ANNEX IV

Mapping of standardization frameworks relevant to cyber supply chain risk management

Figure IV.1. Standardization frameworks relevant to cyber supply chain risk management



RISK ASSESSMENT AND RISK MANAGEMENT STANDARDS

1. ISO/IEC 16085:2006
2. ISO/IEC 27005:2018
3. ISO 28000:2007 and ISO 28001:2007
4. ISO 31000:2018
5. US NIST Framework for Improving Critical Infrastructure Cybersecurity
6. NERC CIP-013-1

PRODUCT AND SERVICE LIFE CYCLE STANDARDS

1. Open Trusted Technology Provider Standard (O-TTPS)
2. ISO/IEC 27034-1:2011/COR 1
3. US NIST Special Publication 800-53, Rev. 4
4. US NIST Special Publication 800-161

INFORMATION SECURITY STANDARDS

1. ISO/IEC 15408 (Common Criteria standard)
2. ISO/IEC 27000 (series of standards)
3. ISO/IEC 27036-1:2014

SYSTEMS ENGINEERING STANDARDS

1. ISO/IEC/IEEE 12207:2017
2. ISO/IEC/IEEE 15288:2015

Note: ICT = information and communications technology; IEC = International Electrotechnical Commission; IEEE = Institute of Electrical and Electronics Engineers; ISO = International Organization for Standardization; NERC = North American Electric Reliability Corporation; NIST = National Institute of Standards and Technology.

ANNEX V

Government and industry-led guidelines and best practices for cyber supply chain risk management

Table V.1. Government and industry-led guidelines and best practices for cyber supply chain risk management

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
1.	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1[55]	US National Institute of Standards and Technology *(government)*	2018 *(Version 1.1. released)*	The framework has grown out of one of the key acts addressing the cybersecurity of US critical infrastructure, adopted under President Obama: *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*, dated 12 February 2013. The executive order was intended to ensure coordination of the critical infrastructure protection policy at the federal level and across different sectors. After the adoption of the executive order, the Cybersecurity Enhancement Act of 2014 updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Using these regulatory provisions as a base, NIST developed its *Framework for Improving Critical Infrastructure Cybersecurity*, widely known as the NIST Cybersecurity Framework. The first version of the framework (1.0) was released in 2015; the current version (1.1) was released in 2018. The framework focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks to be part of an organization's risk management processes. The framework consists of three parts: • The framework core: A set of cybersecurity activities, outcomes and informative references that are common across sectors and critical infrastructure

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				• The implementation tiers: A mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives • The framework profiles: Elements of the core intended to help an organization to align and prioritize its cybersecurity activities with its business or mission requirements, risk tolerances, and resources The framework core is organized into several hierarchical levels of elements, the fundamental one being the five functions required to organize basic cybersecurity activities at their highest level: identify, protect, detect, respond and recover. These five functions are further subdivided into 22 categories and many more subcategories and informative references. The informative references are specific sections of applicable standards, guidelines and practices common among critical infrastructure sectors that illustrate how to achieve the outcomes associated with each subcategory. The list provided in the framework's references covers the majority of international and US national standards and industry practices in the critical infrastructure protection and cybersecurity field, including: • The COBIT (Control Objectives for Information and Related Technologies) framework • ISO/IEC 27000 series (International Organization for Standardization/ International Electrotechnical Commission) • ISO 31000:2009 • ISA/IEC 62443 (International Society of Automation/International Electrotechnical Commission) • NIST Special Publication 800-39

While the framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies and not-for-profit organizations, regardless of their focus or size. The common taxonomy of standards, guidelines and practices that it provides is not country specific. The framework has already been widely used in the United States of America: according to NIST, the framework was used by 30% of US organizations, with a predicted increase to 50% by 2020.[56] Beyond the United States, the framework has been already used by over 20 States.[57] Hence, the framework serves as a de facto global risk-based metastandard tool for organizations in the United States and abroad, allowing them to identify and map cybersecurity standards, best practices and other tools for their specific sector, niche and business process.

With regard to supply chain cybersecurity risk management, major updates and detailed provisions were included in Version 1.1., making this issue one of the major elements of the framework. Thus:

- Section 3.3, "Communicating cybersecurity requirements with stakeholders", was significantly expanded to help users better understand cyber supply chain risk management (SCRM).
- A new Section 3.4, "Buying decisions", highlights the use of the framework in understanding risk associated with commercial off-the-shelf products and services.
- Additional cyber SCRM criteria were added to the implementation tiers.
- A SCRM category, including multiple subcategories, was added to the framework core.

The subcategories for the SCRM category ("ID.SC") of the framework are:

- ID.SC-1: Cyber SCRM processes are identified, established, assessed, managed and agreed to by organizational stakeholders.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				• ID.SC-2: Suppliers and third-party partners of information systems, components and services are identified, prioritized and assessed using a cyber supply chain risk assessment process. • ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity programme and cyber SCRM plan. • ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results or other forms of evaluation to confirm they are meeting their contractual obligations.
2.	US NIST Cyber Supply Chain Risk Management Programme[58]	US National Institute of Standards and Technology *(government)*	2008 *(launched)*	One of the very few governmental activities addressing cyber SCRM through a niche-specific and comprehensive approach. The programme was launched in 2008, when it initiated the development of cyber SCRM practices for non-national security systems in response to Comprehensive National Cybersecurity Initiative No. 11, Develop a Multi-Pronged Approach for Global Supply Chain Risk Management, and has been evolving ever since, reflecting and drawing from new regulatory requirements, standardization developments and broader cybersecurity frameworks (such as the NIST Cybersecurity Framework). Currently, the NIST approach to cyber SCRM includes the following structural blocks:[59] • Foundational practices: Information and communications technology (ICT) SCRM lies at the intersection of information security and supply chain management; existing supply chain and cybersecurity practices provide a foundation for building an effective ICT SCRM programme.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				• Organization-wide: Effective ICT SCRM is an organization-wide activity that involves each organizational tier (organization, mission or business processes, and information systems) and is implemented throughout the system development life cycle. • Risk management process: ICT SCRM should be implemented as part of overall risk management activities, involving identifying and assessing applicable risks, determining appropriate mitigating actions, developing an ICT SCRM plan to document selected mitigating actions, and monitoring performance against that plan. Because ICT supply chains differ across and within organizations, the ICT SCRM plan should be tailored to individual organizational contexts. ○ Risk: ICT supply chain risk is associated with a lack of visibility into, understanding of and control over many of the processes and decisions involved in the development and delivery of ICT products and services acquired by federal agencies. ○ Threats and vulnerabilities: Effectively managing ICT supply chain risks requires a comprehensive view of threats and vulnerabilities. Threats can be either “adversarial” (e.g. tampering, counterfeits) or “non-adversarial” (e.g. poor quality, natural disasters); vulnerabilities may be “internal” (e.g. organizational procedures) or “external” (e.g. part of an organization’s supply chain). • Critical systems: Cost-effective supply chain risk mitigation requires agencies to identify those systems and components that are most vulnerable and will cause the largest organizational impact if compromised.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
3.	Cybersecurity Maturity Model Certification (CMMC), Version 0.6[60]	US Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment *(government)*	Nov emb er 201 9	The CMMC is a mandatory certification process combining various cybersecurity standards, mapping these best practices and processes to maturity levels ranging from basic cyber hygiene to highly advanced practices, and covering cybersecurity in supply chain relations related to the US Defense Industrial Base. The CMMC is supposed to replace the current self-attestation model for US DoD contractors and help the community of Defense Industrial Base suppliers advance towards third-party certification. The certification will be built on existing requirements, such as NIST Special Publication 800-171, NIST Special Publication 800-53 and Aerospace Industries Association (AIA) NAS9933; private sector contributions; and input from academia. This new certification is intended to ensure that existing problems within the Defense Industrial Base will be covered and secure. The CMMC will consist of five levels to measure the cybersecurity practices of contractors.[61]
4.	Supply Chain Security Guidance[62]	UK National Cyber Security Centre *(government)*	November 2018	The aim of the guidance is to provide organizations with an improved awareness of supply chain security, as well as to help raise the baseline level of competence in this regard, through the continued adoption of good practice. The guidance has not been written for organizations with national security (high assurance) requirements and is first and foremost addressed to businesses. The guidance introduces 12 key principles, arranged into four basic stages of addressing security risks in supply chains: 1. Understand the risks: i. Understand what needs to be protected and why. ii. Know who your suppliers are and build an understanding of what their security looks like. iii. Understand the security risk posed by your supply chain.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				2. Establish control: iv. Communicate your view of security needs to your suppliers. v. Set and communicate minimum security requirements for your suppliers. vi. Build security considerations into your contracting processes and require that your suppliers do the same. vii. Meet your own security responsibilities as a supplier and consumer. viii. Raise awareness of security within your supply chain. ix. Provide support for security incidents. 3. Check your arrangements: x. Build assurance activities into your supply chain management. 4. Continuous improvement: xi. Encourage the continuous improvement of security within your supply chain. xii. Build trust with suppliers.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
5.	Cyber Essentials	UK Government in collaboration with private sector *(government / private sector)*	2014	A set of basic technical controls to help organizations protect themselves against common online security threats. The framework was developed by the UK Government in collaboration with the Information Assurance for Small and Medium Enterprises consortium and the Information Security Forum. The full scheme, launched on 5 June 2014, enables organizations to gain one of two Cyber Essentials badges. It is backed by industry, including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organizations offering incentives for businesses. Certification is available at two optional levels: Cyber Essentials and Cyber Essentials Plus. Starting from 1 October 2014, a mandatory governmental requirement has been enforced that requires all suppliers bidding for central governmental contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.[63] The 2017 annual review by the UK National Cyber Security Centre reported that only 7,900 Cyber Essential certificates had been issued since 2014.[64] Some private sector experts attributed this slow uptake to the optional nature of certification (when it is not about meeting requirements for central government supplier contracts).[65]

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
6.	The Cyber/Physical Security Framework (Draft)[66]	Ministry of Economy, Trade and Industry, Japan *(government)*	January 2019 *(draft version issued for public consultation)*	The overarching goal of the framework is "to ensure trustworthiness of a new type of supply chain in 'Society5.0', so-called 'value creation process'". The framework is a major cybersecurity component behind the programme Connected Industries, launched by the Japanese Government to create value by building connections between a wide variety of disparate industrial data. It its turn, Connected Industries is regarded as a major vehicle to implement the goals of a next-generation smart social infrastructure programme, Society 5.0. In terms of structure and basic methodology, the framework is similar to and partially compatible with the US NIST Cybersecurity Framework. Contributing to these goals with a comprehensive framework of applicable standardization tools, requirements and other elements, the regulator (the Ministry of Economy, Trade and Industry) puts digitalized supply chain security in the centre of a new industrial cybersecurity paradigm. In the framework, supply chains in hyperconnected Society 5.0 are understood and described as straddling "both cyber and physical spaces" and changing into "an activity of creating added value that is composed of various dynamically connected items and data". Based on this paradigm, the framework operates with a three-layer approach to understanding the nature and sources of cybersecurity risks to connected industry and to developing measures for their mitigation and prevention. The following layers are identified and used as the underpinning structure of the framework: 1. Connections between organizations: Aims to ensure trustworthiness in the organization's management and to ensure the security of its supply chain.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				2. Mutual connections between cyberspace and physical space: With the advent of Connected Society and cyber–physical industrial infrastructures, the trustworthiness of the value creation process is not ensured unless ensuring the security and reliability of cyber–physical connections and interactions, including data transfer. 3. Connections in cyberspace: To ensure trustworthiness in the value creation process and to create value as intended, the data itself must be trusted. Therefore, data integrity is the basis of trustworthiness. The framework provides the following key elements and tools: 1. Part 1 includes: o The model (the three layers and the six elements) to identify the sources of cybersecurity risk in the value creation process o An outline of the risks and risk sources o Approaches to risk mitigation to ensure trustworthiness 2. In Part 2, using the model provided in Part 1, the risk sources are identified, and policy measures and requirements for their mitigation are presented. 3. In Part 3, the methodological framework and measuring tools for the requirements from Part 2 are provided; in addition, examples of the security measures classified by the strength of security are presented in Appendix C to the framework. The framework is expected to be referred to when an entity that is working on creating added value in the new industrial society, Society5.0, addresses the cybersecurity measures and activities necessary for its

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				business process. In particular, the framework is intended to be used by industry actors to: 1. Identify cybersecurity risk sources relevant for their business and technological processes 2. Formulate a security policy and implement its measures in each enterprise 3. Build a trustworthy chain among each enterprise and across the industry In addition to the *Cyber/Physical Security Framework*, provisions covering third-party cyber risk management were included in the updated Japanese critical infrastructure protection framework *Basic Policy of Critical Information Infrastructure Protection*, revised in 2014. [67] The document includes a section on the promotion of an assessment and certification system for critical information infrastructure protection.[68]
7.	Cyber Security Supply Chain Risk Management Guidance[69]	North American Transmission Forum *(industry / private sector)*	June 2018	The guide aims to summarize best practices for establishing and implementing a cybersecurity SCRM plan, including procurement, specification, vendor requirements and equipment activities. Those best practices include: • Foundational practices: Cybersecurity SCRM requires coordination between SCRM efforts and cybersecurity risk management efforts. Existing cybersecurity and supply chain framework best practices provide a foundation for building an effective cybersecurity risk management strategy. • Organization-wide coordination: Effective cybersecurity SCRM is supported by all layers of the business, including various business functions, and is implemented throughout the system development life cycle.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				• Risk management processes: Cybersecurity SCRM is implemented as part of overall enterprise risk management activities. Execution involves identifying and assessing applicable risks, selecting appropriate mitigating activities, developing a plan to document policies and mitigating activities, and monitoring performance against this plan. Because cybersecurity supply chain risk differs across and within entities, the plan should be tailored to individual organizational contexts. ○ Define criteria: Define cybersecurity supply chain objectives and criteria to assess a supplier’s ability to meet and exceed an entity’s cybersecurity objectives. ○ Evaluate risk: Evaluate supplier risks by obtaining an independent assessment or by obtaining responses to an entity-developed questionnaire describing how the supplier’s business operations and controls for providing Bulk Electric System (BES) cyber systems or related services meet an entity’s cybersecurity criteria and objectives. ○ Respond to risk: Residual risks associated with a supplier’s BES cyber system or related service should be quantified and addressed. Further, entities should periodically reassess cybersecurity supply chain risks presented by existing suppliers and BES cyber systems or related services.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
8.	Software Supply Chain Integrity Framework	Software Assurance Forum for Excellence in Code (SAFECode) *(non-governmental organization / industry / technology community)*	2009 *(initially published)*	SAFECode is a global, industry-led non-profit organization working to increase trust in ICT products and services by promoting availability, awareness and use of more secure and reliable software, hardware and services. The key working areas for the forum are software development, integrity controls and supply chain security. The forum has developed a framework to help organizations select the most appropriate process-based assessment method for evaluating the development process of commercial off-the-shelf product providers when there are no applicable international standards or regulatory guidelines. Members of the forum share commitment to the framework's core principles, aimed at strengthening software assurance.[70] With regard to supply chains, SAFECode's approach and efforts are based on the key provisions and principles of its Software Supply Chain Integrity Framework, initially developed and published in 2009 with contributions from experts from major technology companies (Juniper, Microsoft, Nokia, SAP, Symantec).[71] The framework focuses on software supply chains and their assurance, regarding the latter as a responsibility shared among suppliers (vendors), service or solution providers, and customers, and encompassing three areas: security, authenticity and integrity. The framework's primary aim is to provide the industry actors with better guidelines and vision to ensure the integrity of their software supply chains. According to the framework, software supply chain integrity controls derive from the following security and integrity principles:[72] ○ Chain of custody: Each change and handoff made during the source code's lifetime is authorized, transparent and verifiable. ○ Least privilege access: Personnel can access critical data with only the privileges needed to do their jobs.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				○ Separation of duties: Personnel cannot unilaterally change data nor unilaterally control the development process. ○ Tamper resistance and evidence: Attempts to tamper are obstructed, and when they occur, they are evident and reversible. ○ Persistent protection: Critical data are protected in ways that remain effective even if removed from the development location. ○ Compliance management: The success of the protections can be continually and independently confirmed. ○ Code testing and verification: Methods for code inspection are applied, and suspicious code is detected. The framework focuses on software supply chains only, although it mentions and addresses security and integrity challenges related to software embedded into hardware. Thus, it does not cover 100% of the ICT or technology supply chain in terms of its scope and applicable practices. However, SAFECode has produced additional guidelines and publications that focus on supply chain assurance in addition to its 2009 framework. Those include *Overview of Software Integrity Controls*, *Principles for Software Assurance Assessment*, and *Managing Security Risks Inherent in the Use of Third-party Components.* [73] Currently, those publications, as well as the principles and best practices they encompass, are discussed, promoted and developed by SAFECode's 16 members, including technology giants such as Boeing, Huawei, Intel, Microsoft, Siemens and Symantec.[74]

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
9.	Deliver Uncompromised– A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War[75]	The MITRE Corporation *(private sector/ technical community)*	2018	The report addresses the challenges posed by the changing nature of warfare, including blended operations, the development of ICT and other factors that the US DoD and the intelligence community have been facing with regard to ensuring the security and integrity of their cyber supply chains. Thus, the scope of the publication and its recommendations is limited to a specific sector of the US Defense Industrial Base, with particular focus on the DoD. However, within this niche, the report provides quite comprehensive multi-tier analysis covering legislation and regulation, policy and administration, acquisition and oversight, and programmes and technology. The report identifies 15 courses of action, which are presented for the near, medium and long terms, recognizing the need for immediate action coupled with a long-term commitment and strategy. Also, the courses of action provided in the report de facto span beyond supply chain security management in the US defence and intelligence sector to address the practices, security management models and processes of private enterprises. This responds to the deep and inherent cross-sectoral ties and interconnections in the ICT industry, as the report stresses that supply chain vulnerability extends well beyond the DoD, across government and into the private sector. The 15 courses of action identified in the report are:[76] 1. Elevate security as a primary metric in DoD acquisition and sustainment. 2. Form a whole-of-government National Supply Chain Intelligence Center. 3. Execute a campaign for education, awareness and ownership of risk.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				4. Identify and empower a chain of command for supply chains, with accountability for security and integrity to the US Deputy Secretary of Defense. 5. Centralize the Supply Chain Risk Management – Threat Analysis Cell with the industrial security or critical infrastructure mission owner under the Defense Security Service, and extend its authority. 6. Increase DoD leadership recognition and awareness of asymmetric warfare via blended operations. 7. Establish independently implemented automated assessment and continuous monitoring of Defense Industrial Base software. 8. Advocate for litigation reform and liability protection. 9. Ensure supplier security and use contract terms. 10. Extend the 2015 National Defense Authorization Act Section 841 authorities for "Never contract with the enemy". 11. Institute innovative protection of DoD system design and operational information. 12. Institute industry-standard ICT practices in all software developments. 13. Require vulnerability monitoring, coordinating and sharing across the supply chain of command. 14. Advocate for tax incentives and private insurance initiatives. 15. For resilience, employ failsafe mechanisms to backstop mission assurance.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
10.	Cyber Product International Certification (CPIC) Commission Initiative[77]	Electric Infrastructure Security (EIS) Council *(industry / private sector)*	June 2018 *(draft proposal published)*	The initiative aims to provide electric infrastructure operators in the United States with a comprehensive, stakeholder-driven process to certify that crucial hardware and software products are even minimally scrubbed of malware and other means of adversary exploitation. In particular, the initiative should provide added value to governmental efforts in ensuring the security and resilience of critical supply chains through establishing a voluntary, demand-driven business model to incentivize vendors to secure selected segments of their hardware and software product portfolios against corruption. The action items and key issues to be addressed by the initiative, according to its business model, are: 1. Leveraging existing company plans and capabilities for SCRM. 2. Enabling the centralized cross-sector coordination of efforts and activities to incentivize, develop and implement more comprehensive certification and validation processes for SCRM than those considered practical today. 3. Guarding against "minimalist" standards, because standards that constitute the minimum required SCRM measures are not sufficient to ensure the security of global supply chains. Instead, a non-regulatory approach, focused on certification of best practices, rather than minimalist, broad-brush standards, should be leveraged and employed across industries. 4. Internationalizing the initiative through promotion and global industry events in order to develop to a certification process that will be applied to the full, international footprint of modern digitalized supply chains.

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				5. Developing a tiered certification system, including basic level and prime certification level, both going beyond the minimal set of requirements codified in (inter-)national standards. 6. Incentivizing and developing governmental participation in the initiative, both domestic and international, to increase the added value of the initiative and its outreach and ensure that it would be maximally compatible with participating government stakeholders' own needs. 7. Developing a charter of the initiative and opening it for participation to interested stakeholders.
11.	Purchasing Secure ICT Products and Services: A Buyers Guide, Version 1.0[78]	EastWest Institute and technology sector companies *(academia / private sector)*	2016 *(published)*	The guide aims to provide a compendium of best practices and guidelines for organizations (including both buyers and sellers of ICT products) as well as for users and is intended to help them better understand and address the cybersecurity and privacy risks related to ICT products and services and their supply chains. In terms of methodology, the publication reflects and draws from some industry best practices. Thus, the approach suggested by the guide is based on a set of specific questions that managers at enterprises and users of ICT products should address to minimize security risks when developing, purchasing, selling or using ICT products. This set of 25 questions was adapted and combined from the 11 categories of questions contained in the 2014 report by Huawei, summarizing requirements to meet and questions to address to ensure end-to-end cybersecurity in relationships with vendors.[79] Thus, the EastWest Institute report aims to build on and extrapolate some of the already deployed industry practices (although first and foremost on the US market and within the US

regulatory and standardization landscape), rather than develop best practices and recommendations from scratch.

The guide's framing questions are broken into three major categories, with further details of major aspects and niches of action:[80]

- Enterprise security governance:
    - Strategy and control
    - Standards and processes
    - Human resources
- Product and services life cycle – from design through sustainment and response:
    - Design and development
    - Build (ICT product compilation and manufacturing process)
    - Release, fulfilment and distribution
    - Sustainment and response
    - Sourcing and supply chain
- Creating assurance:
    - Fostering assurance
    - Demonstrating assurance

Specifically for supply chains, the guide aims to cover all related aspects, including the selection and authorization of suppliers and business partners, such as original equipment manufacturers, component suppliers, integrators, value added resellers and distributors; the protection of the suppliers' environment (e.g. physical and logical access control); and the security and integrity of the manufacturing processes (e.g. practices, training and tooling for secure transmission and handling, open source, counterfeit mitigation, and malware detection). The key issues to address within this context, accentuated through the guide's questions, include:

NO.	FRAMEWORK / MECHANISM	ORGANIZATION (TYPE)	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				• The necessity of security evaluations of third-party inputs before their selection, and their tracking and validation on entering the supply chain • The quality and efficiency of the security management of an enterprise's ICT suppliers, including establishing relevant security criteria and passing them on to suppliers • Describing and assessing upstream and downstream manufacturing process flow to discover the existence of any tainted or counterfeit ICT components

ANNEX VI

Examples of technology sector corporate supply chain assurance frameworks

Table VI.1. Examples of technology sector corporate supply chain assurance frameworks

NO.	COMPANY	FRAMEWORK	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
1.	Microsoft	Supply Chain Assurance Framework[81]	2017 *(being updated)*	Supplier assessment framework*:* The framework uses a combination of supplier risk profiling and focused control-based assessments, including: • Risk indicators • Scoring • Risk profile • Recommended courses of action Policies, standards and control procedures: The company has developed policies, standards and control procedures for software, goods and services from third-party suppliers. These policies map to industry regulations and authoritative sources (e.g. US National Institute of Standards and Technology [NIST] Cybersecurity Framework or relevant International Organization for Standardization [ISO]/ International Electrotechnical Commission [IEC] standards), thus helping Microsoft meet external and internal security obligations. Security technical control procedures are key tools, developed to provide detailed steps to follow for Microsoft's specific technologies or processes. Supplier risk profiling model: Microsoft has developed a dashboard containing at-a-glance information about each supplier and the health of the products or services they offer to the company. The information about suppliers is pulled from multiple sources and arranged in standardized categories on the dashboard. Each supplier's profile is scored for risk on the basis of Microsoft's experience with past purchases.

				This score helps Microsoft determine how much more assessment is needed to grant confidence in a supplier’s product or service. Integrating assurance into the procurement life cycle: The Supply Chain Assurance Program integrates security escalations to ensure that Microsoft chooses secure third-party software, goods and services from trusted suppliers. Currently, the programme governs three supplier services: • Third-party software • Solution integrators (suppliers that provide staff augmentation and consulting services to Microsoft) • Factories building components and products for Microsoft With regard to these three elements, Microsoft’s approach implies integration of assurance into all stages of the procurement life cycle, including: 1. Pre-selection of supplier 2. Selection of supplier, based on attestation procedure (security reviews of the supplier) and relevant attestation requirements. 3. Contracting with the supplier 4. Ongoing monitoring, including during the post-contracting stage Measuring customer satisfaction and programme health: Developing and using specific performance indicators to measure adoption, performance and customer satisfaction. Addressing security in the future: Permanently developing, updating and expanding supply chain assurance and its scope and functionality. Mechanisms from the framework and the programme are used across different niches of Microsoft’s supply chain. For example, in the Assuring the Security of Cloud Services Framework,[82] compromise of the cloud service provider supply chain is addressed among key risks to cloud security. With regard to aligned security control procedures, supply chain integrity processes are mentioned.[83]

NO.	COMPANY	FRAMEWORK	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
2.	Kaspersky	Global Transparency Initiative (GTI)[84]	2017 *(launched)*	The GTI aims to engage the broader information security community and other stakeholders in validating and verifying the trustworthiness of its products, internal processes and business operations. It also introduces additional accountability mechanisms by which the company can further demonstrate that it addresses any security issues promptly and thoroughly. Key measures implemented as elements of the initiative include: • Opening access to independent review of Kaspersky's source code, software updates and threat detection rules to governments and accredited experts on request. • Opening access to independent review of Kaspersky's secure development life cycle processes, and its software and supply chain risk mitigation strategies. • Global deployment of Kaspersky's corporate Transparency Centers (TCs) to address any security concerns, together with customers, trusted partners and government stakeholders. The TCs are non-profit organizations qualified to conduct technical software reviews, including independent third-party reviews of Kaspersky's products (including pieces of their source code). The TCs serve as key institutional infrastructure for the GTI and an interface for interaction with third-party reviewers of Kaspersky's ICT products. Also, importantly, Kaspersky started to relocate its users' data and its processing from data centres in the Russian Federation to its new TCs. The company aims to have at least three TCs operating in different regions by 2020: ○ The first TC was opened in Zurich, Switzerland, in November 2018 and serves as a facility for such partners to access company code reviews, software updates and threat detection rules, along with other activities.[85] ○ The second TC was launched in Madrid in June 2019.[86] ○ By early 2020, the company plans to open its third TC in Kuala Lumpur, expanding its initiative to Asia Pacific.[87]

NO.	COMPANY	FRAMEWORK	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				• Increased bug bounty rewards up to $100,000 for critical vulnerabilities found under Kaspersky's Coordinated Vulnerability Disclosure programme. • Also, linked to the launch of GTI, Kaspersky has passed an independent external audit against the Service Organization Control (SOC) 2 reporting framework.[88] The audit was conducted by one of the Big Four consulting companies; the report was published on Kaspersky's website.[89] In addition to and in connection with GTI, Kaspersky published the results of a voluntary third-party legal assessment aimed at providing an independent evaluation of the obligations the company adheres to in line with Russian legislation.[90] Although the scope and objectives of the GTI do not exclusively focus on supply chain risk management (SCRM) or explicitly mention it, its framework serves as a de facto downstream supply chain assurance vehicle, allowing Kaspersky to demonstrate the absence of hidden functions in its products to its customers and regulators in national markets. This could be supported by the fact that the UK National Cyber Security Centre (NCSC) guidance addresses the risks associated with the procurement and use of Kaspersky's products specifically in the context of SCRM.[91] Moreover, the GTI framework's design and scope seem to match the criteria for potential security assurance solutions mentioned in the NCSC guidance.[92]

3.	Huawei	1. Supply Chain Management programme 2. Cyber Security Evaluation Centre framework	1. At least since 2013 2. At least since 2010	Huawei has been developing a comprehensive company-wide approach encompassing security assurance of its products and its business processes. The approach was discussed in the company's 2013 white paper,[93] with its key components and pillars identified and presented in some detail: • A company-wide coordinated approach to security assurance. A central body – Huawei's Global Cyber Security Committee – was granted responsibility over Huawei's security assurance programme, including its ratification, strategic planning, policies, road map and investment, as well as the strategy's implementation, resolution of conflicting strategic priorities, and auditing.[94] Activities of this central entity have been also supported by a set of entities and management positions on lower layers of the corporate hierarchy, including the company's Global Cyber Security Officer, Global Cyber Security Office, and Regional and Departmental Cyber Security Officers. • Integration of security assurance throughout the company's business processes, including research and development (R&D), the supply chain, sales and marketing, delivery, and technical services. Thus, supply chain security assurance, including cyber SCRM, has been regarded and deployed by the company not as an isolated or ad hoc security management niche, but as another element in this comprehensive effort. • Major focus on national and international standardization and certification frameworks as key tools for company-wide security assurance and relations with customers, contractors and suppliers. This covers such processes as conducting internal auditing and receiving external certification and auditing from security authorities and independent third-party agencies. According to the company's reports and white papers, its security assurance for these processes includes the use of and compliance with such international standards as ISO 9001, ISO 14001, Occupational Health and Safety Assessment Series (OHSAS) 18001, ISO 26000, ISO 27001, ISO 15408, the Customs Trade Partnership Against Terrorism, and Transport Asset Protection Association (TAPA) 11.[95]

- Standardized process frameworks and tiered responsibility for and coordination of the totality of the company's internal processes, ranging from regulatory compliance and workforce management to R&D, market management, product configuration management, and the manufacturing cycle.

With regard to corporate supply chain security assurance, the Huawei Supply Chain Management programme is based on several quality control and process management frameworks and activities, including Six Sigma, optimization projects, quality control circles, the traditional suggestion box and the Huawei Production System.[96]

- Since the beginning of the 2000s, the company's efforts in addressing supply chain security assurance have been developing along three key vectors:
    1. Extended quality control and security assurance activities from internal product quality to external customer relationships.
    2. Extension of SCRM activities from the production process to the end-to-end supply chain process (including processes related to planning, acquisition management, etc.).
    3. Increased and more comprehensive reliance on and compliance with international standards of process management, quality control, cybersecurity and, particularly, SCRM. Prioritized standardization frameworks, including the aforementioned series of ISO/IEC standards, as well as US NIST Cybersecurity Framework[97] and the Open Trusted Technology Provider Standard.[98]

In particular, on the basis of the ISO 28000 standard,[99] Huawei has developed its internal Supplier Cyber Security System Qualification Standard to serve as an underpinning pillar for a company-wide comprehensive supplier management system. The system is intended to identify and control security risks during the end-to-end process, from incoming materials to custom delivery. In particular, the system uses a detailed system of indicators and weights (10 items and 49 questions), which are applied to each contractor or vendor part of the supply chain.[100]

Additional mechanisms deployed by the company to address internal supply chain security risks, with major cybersecurity components, include:

- Supply Chain Cyber Security Baseline framework, covering requirements on physical security (entity delivery security); software delivery security; and organizational, process and personnel security awareness[101]
- An end-to-end traceability chain in the software delivery system, based on the use of barcode identifiers of all products and components coming through corporate supply chains and covering material acceptance, material distribution, printed circuit board assembly and testing, whole equipment assembly and testing, packaging, and transportation and regional delivery[102]

In parallel with developing internal quality control and SCRM mechanisms, the company's major efforts since the early 2000s have been also aimed at creating frameworks to provide customer (external) security assurance and ensure trust in its products among users, partners and governmental authorities in the company's major markets. One of the key efforts in this direction was the establishment of the Huawei Cyber Security Evaluation Centre (HCSEC) in November 2010 in Banbury, United Kingdom, under a set of arrangements between Huawei and the UK Government. The HCSEC's function is to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK critical national infrastructure through such actions as:[103]

- Providing security evaluation for Huawei products used in the UK telecommunications market
- Providing insights into Huawei's UK strategies and product ranges to the UK Government
- Cooperating and communicating with the UK NCSC, the national technical authority for information assurance and the lead Government operational agency on cybersecurity, which is in charge of dealing with HCSEC, and with Huawei more generally, on technical security matters on behalf of the UK Government

The oversight over the HCSEC and, in a broader sense, cybersecurity issues with Huawei products shipped to the UK market, is conducted through the mechanisms of the HCSEC Oversight Board, established in 2014 and chaired by the Chief Executive Officer of the NCSC and an executive member of the Government Communications Headquarters Board with responsibility for cybersecurity. The last report to the UK National Security Adviser was completed by the HCSEC Oversight Board in March 2019.[104]

As of today, this assurance framework has demonstrated some controversial results. According to the HCSEC Oversight Board report of 2019, "no material progress has been made on the issues raised in the previous 2018 report",[105] referring to "shortcomings in Huawei's engineering processes" that have "exposed new risks in the UK telecommunication networks and long-term challenges in mitigation and management".[106] The 2019 report's publication coincided with a wave of increased attention from regulators and policy authorities due to Huawei expansion into the US and European markets, especially in the 5G equipment segment. That led to the interpretation of the report by the media and experts[107] as another case in the increasingly serious trust issues that Huawei has been facing in the West, and to possible regulatory moves by some governments to limit Huawei products' access to their technology market's sensitive niches. The 2018 report, indicating significant issues with the security of Huawei's products shipped to the UK market, also praised the efficiency of the HCSEC framework itself, stating that it "provides unique, world class cyber security expertise" to assist the UK Government efforts.[108]

Despite security concerns raised by the UK regulators based on their work with the HCSEC framework, Huawei has been expanding its approach to customer security assurance and trust building in the markets of continental Europe. In March 2019, the company launched its Cyber Security Transparency Centre in Brussels, linking this effort to its call for industry and government to establish unified, objective cybersecurity standards.[109] According to the company, the centre in Brussels has three major functions:[110]

1. Showcase Huawei's end-to-end cybersecurity practices, from strategies and supply chains, to R&D and products and solutions.

NO.	COMPANY	FRAMEWORK	YEAR (STATUS)	SUMMARY OF KEY PROVISIONS
				2. Facilitate communication between Huawei and key stakeholders on cybersecurity strategies and end-to-end cybersecurity and privacy protection practices, including cybersecurity standardization. 3. Provide a product security testing and verification platform and related services to Huawei customers.

ANNEX VII

(Self-)assessment and auditing tools for cyber supply chain risk management

Table VII.1. (Self-)assessment and auditing tools for cyber supply chain risk management

NO.	TOOL	DEVELOPER / AUTHOR	TARGET AUDIENCE	SUMMARY OF KEY PROVISIONS AND COMMENTS
1.	Exostar's Risk Management Solution[111]	Exostar	US aerospace sector companies, defence contractors and other highly regulated industrial enterprises	Exostar was established in 2000 as a joint venture between five of the largest US and UK aerospace and defence companies: Boeing, BAE Systems, Lockheed Martin, Raytheon and Rolls Royce. Exostar initially functioned as a supply chain portal to bring together buyers and sellers in the aerospace industry. Over the years, it has evolved into a cloud-based, online platform for secure enterprise and supply chain collaboration among defence contractors from the aerospace industry, as well as other highly regulated industries. Currently, it functions as an online platform enabling organizations to assess, measure and mitigate risk in real time across multi-tier partner and supplier networks, with a considerable focus on cybersecurity risks. [112] In particular, the solution enables organizations to track and measure the vulnerability and compliance status of their partners and suppliers, for example federal prime defence contractors who need to address the specific requirements included in the governmental regulations. In combination with other Exostar platform tools (Supply Chain Collaboration and Management, Secure Collaboration),[113] the Exostar service aims to create an ecosystem for end-to-end traceability and risk assessment of supply chains across networks of suppliers and partners of its users.

NO.	TOOL	DEVELOPER / AUTHOR	TARGET AUDIENCE	SUMMARY OF KEY PROVISIONS AND COMMENTS
2.	Vendor Cybersecurity Tool[114]	Rivial Security	Private enterprises, mostly in the US market	This is a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identity improvement opportunities in the context of their overall organizational performance. As such, it mostly addresses the issues of vendor due diligence and does not have an exclusive focus on supply chain risk management (SCRM) for information and communications technology (ICT).
3.	CyberChain Portal-Based Assessment Tool[115]	University of Maryland, Robert H. Smith School of Business, Supply Chain Management Center	Enterprises seeking assessment in implementing the US National Institute of Standards and Technology (NIST) Cybersecurity Framework	This tool provides guidelines to measure and assess cyber supply chain risk. It was designed and developed as a companion assessment tool for enterprises to use in implementing practices from the US NIST Cybersecurity Framework. It has a specific focus on SCRM in accordance with corresponding provisions of the US NIST Cybersecurity Framework.
4.	SecurityScorecard[116]	InfoGuard / SecurityScorecard	Local (Swiss) and European enterprises and private businesses	This is an online platform enabling users to view and continuously monitor security ratings, add vendors or partner organizations, and report on the cyberhealth of their supply chain, or their third-party ecosystem in a broader sense.

NO.	TOOL	DEVELOPER / AUTHOR	TARGET AUDIENCE	SUMMARY OF KEY PROVISIONS AND COMMENTS
5.	Vendor Application Security Testing[117]	VeraCode	Private enterprises and other entities using online applications (apps) and third-party app ecosystems	This is an online cloud-based tool aiming to reduce the risk associated with third-party software, mostly in the niche of application security. The tool is designed to manage a company's entire third-party programme as a cloud-based service and work directly with vendors in the client's software supply chain to ensure they are compliant with its corporate security policies.
6.	BitSight for Third-Party Risk Management[118]	BitSight	Private enterprises with third-party ICT supplier–contractor relationships	This tool aims to deliver a comprehensive tool for third-party cybersecurity risk management for enterprises. It is designed as an automated tool to continuously measure and monitor the security performance of vendors and identify related cybersecurity risks. It also allows for a collaboration regime when an enterprise uses it to develop and coordinate its cybersecurity SCRM programme in collaboration with its vendors.
7.	Baldrige Cybersecurity Excellence Builder, Version 1.1[119]	US National Institute of Standards and Technology	Leaders and managers: senior leaders, chief security officers and chief information officers	This is a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organizational performance. It does not have exclusive focus on cybersecurity SCRM, but it addresses third-party and vendor-related cybersecurity risks as a separate category. It is available for business, non-profit, education and health-care sectors.

ANNEX VIII

International and multi-stakeholder normative initiatives addressing supply chain security and integrity

Table VIII.1. International and multi-stakeholder normative initiatives addressing supply chain security and integrity

NO.	ENTITY (ORGANIZATION / FRAMEWORK)	SOURCE	YEAR PUBLISHED / ADOPTED	PROVISIONS
STATES AND INTERGOVERNMENTAL FORUMS				
1.	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98*)[120]	2013	Threats, risks and vulnerabilities: "8. States are concerned that embedding harmful hidden functions in [information and communications technologies (ICTs)] could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security." III. Recommendations on norms, rules and principles of responsible behaviour by States: "24. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services.

NO.	ENTITY (ORGANIZATION / FRAMEWORK)	SOURCE	YEAR PUBLISHED / ADOPTED	PROVISIONS
				"25. Member States should consider how best to cooperate in implementing the above norms and principles of responsible behaviour, including the role that may be played by private sector and civil society organizations. These norms and principles complement the work of the United Nations and regional groups and are the basis for further work to build confidence and trust."
2.		Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)[121]	2015	III. Norms, rules and principles for the responsible behaviour of States: "13. (i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."
3.		Impressions of the Chairman of the 5th Group of Governmental Experts on Developments in the	2016–17	"Take steps to prevent non-state actors, including the private sector, from using harmful hidden functions for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory.

NO.	ENTITY (ORGANIZATION / FRAMEWORK)	SOURCE	YEAR PUBLISHED / ADOPTED	PROVISIONS
		Field of Information and Telecommunications in the Context of International Security (2016–2017)[122]		"Identify trust-building measures that can help allay concerns about harmful hidden functions in ICT products, encouraging the private sector and civil society to play an appropriate role to this end."
4.	Group of Seven (G7)	Dinard Declaration on the Cyber Norm Initiative, G7/8 Foreign Ministers Meeting[123]	2019	Supply chain issues are not directly mentioned in the Cyber Norm Initiative. However, the document recalls all norms from the United Nations Group of Governmental Experts 2010, 2013 and 2015 reports, which include the supply chain norms. The G7 States committed to: • "Encourage better and increased voluntary exchange of information, among ourselves and with others, on the steps taken by our respective states to understand and effectively implement the voluntary, non-binding norms of responsible state behavior in cyberspace and the recommendations contained in the abovementioned reports; • Share the best practices and lessons learned that will be identified as a result of this process with a wide range of states and other stakeholders; • Engage with other states to include them in our peer-learning, cooperative, transparency and confidence-building efforts;

NO.	ENTITY (ORGANIZATION / FRAMEWORK)	SOURCE	YEAR PUBLISHED / ADOPTED	PROVISIONS
				- Cooperate to help build our partners' capability to implement the above-mentioned voluntary, non-binding norms and recommendations."
5.	Shanghai Cooperation Organisation	International Code of Conduct for Information Security[124]	2015	"Each State voluntarily subscribing to this Code of Conduct pledges: … "(5) To endeavour to ensure the supply chain security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and communications networks to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security."
MULTI-STAKEHOLDER NORMATIVE FRAMEWORKS AND INITIATIVES				
6.	Digital Geneva Convention to Protect Cyberspace (Microsoft)	A Digital Geneva Convention to Protect Cyberspace[125]	2017	States should be committed to: "Refrain from inserting or requiring 'backdoors' in mass-market commercial technology products."
7.	Cybersecurity Tech Accord (Microsoft)	Cybersecurity Tech Accord – Protecting Users and Customers Everywhere[126]	2018	"2. We will oppose cyberattacks on innocent citizens and enterprises from anywhere.

NO.	ENTITY (ORGANIZATION / FRAMEWORK)	SOURCE	YEAR PUBLISHED / ADOPTED	PROVISIONS
				• We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.”
8.	Charter of Trust (launched by Siemens AG)	Charter of Trust[127]	2018 / 2019	“**2 Responsibility throughout the digital supply chain**[128] “Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all [Internet of Things (IoT)] layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards, such as: • **Identity and access management:** Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them. • **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes wherever appropriate. • **Continuous protection:** Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism.” “**7 Certification for critical infrastructure and solutions**

NO.	ENTITY (ORGANIZATION / FRAMEWORK)	SOURCE	YEAR PUBLISHED / ADOPTED	PROVISIONS
				"Companies – and if necessary – governments establish mandatory independent third-party certification (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions." Starting on February 15, 2019, new Siemens suppliers must comply with minimum binding cybersecurity requirements, which are being introduced step by step and anchored in a separate, binding clause in all new contracts. Baseline binding requirements introduced by Siemens as part of the Charter of Trust initiative to strengthen cybersecurity throughout all digital supply chains include:[129,130] • Data shall be protected from unauthorized access throughout the data life cycle. • An appropriate level of identity and access control and monitoring, including of third parties, shall be in place and enforced. • A process shall be in place to ensure that products and services are authentic and identifiable. • A minimum level of security education and training for employees shall be regularly deployed.
9.	Global Commission on the Stability of Cyberspace (GCSC)	Norm Package Singapore[131]	2018	"2. Norm to Avoid Tampering …

NO.	ENTITY (ORGANIZATION / FRAMEWORK)	SOURCE	YEAR PUBLISHED / ADOPTED	PROVISIONS
				"State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace."
10.	Paris Call for Trust and Security in Cyberspace	Paris Call for Trust and Security in Cyberspace[132]	February 2018 / February 2019	"Willingness to work together...to: ... – Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain; ... – Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace."

ENDNOTES

[1] Nissen et al. (2019).
[2] US NIST (2013).
[3] Karygiannis et al. (2007).
[4] ISO (2014).
[5] ENISA (2015).
[6] ACSC (2019).
[7] The Open Group (2019).
[8] The Open Group (2017).
[9] US NIST (2015a).
[10] CNSS (2015).
[11] Heinbockel et al. (2017). Original quote from: M. Reed, J. F. Miller and P. Popick, "Supply Chain Attack Patterns: Framework and Catalog," 2014.
[12] US NIST (2015b).
[13] US NIST (2018a).
[14] NERC (2018).
[15] Oldehoeft (1992).
[16] See: Cisco (2017); Microsoft Security Intelligence (2017).
[17] US NIST (2017).
[18] See also: Greenberg (2018); TrendLabs (2017).
[19] See: Kaspersky (2019b); Zetter (2019).
[20] Microsoft Defender ATP Research Team (2018).
[21] ISO (2006).
[22] ISO (2018b).
[23] See: ISO (2018c).
[24] ISO (2007a).
[25] ISO (2007b).
[26] ISO (2018a).
[27] See: Common Criteria (2019d).
[28] See: Common Criteria (2019c).
[29] See: Common Criteria (2019b).
[30] See: Common Criteria (2019a).
[31] ISO (2019).
[32] See: ISO (2013).
[33] ISO (2014).
[34] ISO (2014).
[35] See: ENISA (2015).
[36] ISO (2017).
[37] ISO (2015b).
[38] The Open Group (2015b).
[39] See: The Open Group (2015a); ISO (2015a).
[40] See: 114th United States Congress (2015).
[41] See: ISO (2018d).
[42] ISO (2018d).
[43] See: The Open Group (2017).
[44] NERC (2018).
[45] See: FERC (2016).
[46] FERC (2016).
[47] SAE International (2012).
[48] SAE International (2019).
[49] SAE International (2012).
[50] SEMI (2009).
[51] SEMI (2014).
[52] GSMA (2019).

[53] EC (2019a).
[54] EC (2019b).
[55] US NIST (2018a).
[56] US NIST (2018b).
[57] US NIST (2018b).
[58] US NIST (2018c).
[59] See: US NIST (2018c); US NIST (2019a).
[60] Office of the Under Secretary of Defense for Acquisition and Sustainment (2019).
[61] Exostar (2019c).
[62] NCSC (2018).
[63] See: Crown Commercial Service (2014).
[64] NCSC (2017).
[65] NCSC (2018).
[66] METI (2019).
[67] Information Security Policy Council (2014).
[68] Information Security Policy Council (2014, 31, para. 5.3.4).
[69] NATF (2018).
[70] SAFECode (2019c).
[71] SAFECode (2009).
[72] SAFECode (2009).
[73] See: SAFECode (2019b).
[74] See: SAFECode (2019a).
[75] Nissen et al. (2019).
[76] Nissen et al. (2019).
[77] See: Stockton (2018).
[78] EastWest Institute (2016).
[79] See: Suffolk (2014).
[80] EastWest Institute (2016).
[81] See: Microsoft (2017).
[82] Kavanagh (2017).
[83] Kavanagh (2017).
[84] See: Kaspersky (2019c).
[85] Kaspersky (2019c).
[86] BusinessWire (2019).
[87] Barbaschow (2019).
[88] See more: PwC (2019).
[89] Kaspersky (2019a).
[90] See: Hober (2019).
[91] Martin (2018).
[92] Martin (2018). In particular, the guidance refers to ongoing discussions with Kaspersky concerning the opportunity to "develop a framework that we and others can independently verify, which would give the Government assurance about the security of their involvement in the wider UK market".
[93] See: Suffolk (2013).
[94] Suffolk (2013, 11).
[95] See also: Purdy (2016).
[96] Purdy (2016, 20–1).
[97] See Annex V, bullet point 1 for details.
[98] See Annex III, bullet point 10 for details.
[99] ISO 28000:2007 and ISO 28001:2007. See Annex III, bullet point 3 for details.
[100] Purdy (2016, 21).
[101] Purdy (2016, 22–3).
[102] Purdy (2016).
[103] See: HCSEC Oversight Board (2019).
[104] HCSEC Oversight Board (2019).
[105] HCSEC Oversight Board (2019).
[106] HCSEC Oversight Board (2018).

[107] See: Bond & Fildes (2019); Porter (2019); Sweney (2019).
[108] See: HCSEC Oversight Board (2018, 17).
[109] Huawei (2019).
[110] Huawei (2019).
[111] Exostar (2019a).
[112] See: US NIST (2019b).
[113] See: Exostar (2019b).
[114] Lindberg (2018).
[115] Robert H. Smith School of Business (2015).
[116] Security Scorecard (2019).
[117] VeraCode (n.d.).
[118] BitSight (2019).
[119] Baldrige Cybersecurity Initiative (2019).
[120] UNGA (2013).
[121] UNGA (2015b).
[122] See: Tikk & Kerttunen (2018, 50).
[123] G7/8 Foreign Ministers Meetings (2019).
[124] UNGA (2015a).
[125] Microsoft (2018).
[126] Cybersecurity Tech Accord (2019).
[127] Siemens AG (2019a).
[128] Siemens AG (2019b).
[129] Siemens et al. (2019).
[130] Siemens AG (2019c).
[131] GCSC (2018).
[132] France Diplomatie (2018).

REFERENCES

114th United States Congress (2015–2016). 2015. *National Defense Authorization Act for Fiscal Year 2016.* As of 10 November 2019: https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf

Australian Cyber Security Centre (ACSC). 2019. *Cyber Supply Chain Risk Management – Practitioners Guide*. As of 10 November 2019: https://www.cyber.gov.au/sites/default/files/2019-06/Supply%20Chain%20Risk%20Management%20-%20Practitioners%20guide.pdf

Baldrige Cybersecurity Initiative. 2019. *Baldrige Cybersecurity Excellence Builder*. Version 1.1. Gaithersburg: US National Institute of Standards and Technology. As of 10 November 2019: https://www.nist.gov/system/files/documents/2019/03/24/baldrige-cybersecurity-excellence-builder-v1.1.pdf

Barbaschow, Asha. 2019. 'Kaspersky Touts APAC Transparency Center as Proving 100% Trustworthiness'. ZDNet, 16 August, 1.44 a.m. GMT. As of 10 November 2019: https://www.zdnet.com/article/kaspersky-touts-apac-transparency-center-as-proving-100-trustworthiness

BitSight. 2019. 'BitSight for Third-Party Risk Management'. As of 10 November: https://www.bitsight.com/security-ratings-vendor-risk-management

Bond, David, & Nic Fildes. 2019. 'UK Intelligence Panel Warns on Huawei Security Flaws. Damning Report Backs US Doubts on Chinese Telecoms Company's Ability to Fix Problems'. *Financial Times*, 28 March. As of 10 November 2019: https://www.ft.com/content/8d701096-50ac-11e9-b401-8d9ef1626294

BusinessWire. 2019. 'Kaspersky Lab Opens New Transparency Center in Madrid and Conducts Independent Legal Assessment of Russian Legislation Related to Data Processing'. BusinessWire.com, 2 April, 10.24 a.m. EDT. As of 10 November 2019: https://www.businesswire.com/news/home/20190402005727/en/Kaspersky-Lab-Opens-New-Transparency-Center-Madrid

Cisco. 2017. 'CCleanup: A Vast Number of Machines at Risk'. Cisco TALOS, 18 September. As of 10 November 2019: https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

Committee on National Security Systems (CNSS). 2015. *Committee on National Security Systems (CNSS) Glossary*. CNSSI No. 4009. Ft Meade: CNSS Secretariat. As of 10 November 2019: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Common Criteria. 2019a. 'Licensed Laboratories'. Common Criteria Portal. As of 10 November: https://www.commoncriteriaportal.org/labs

———. 2019b. 'Members of the CCRA'. The Common Criteria Portal. As of 10 November: https://www.commoncriteriaportal.org/ccra/members

———. 2019c. 'Protection Profiles'. The Common Criteria Portal. As of 10 November: https://www.commoncriteriaportal.org/pps

———. 2019d. 'The Common Criteria'. The Common Criteria Portal. As of 10 November: https://www.commoncriteriaportal.org

Crown Commercial Service. 2014. *Procurement Policy Note – Cyber Essentials Scheme*. Action Note 09/14. Gov.uk, 26 September. As of 10 November 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/526200/ppn_update_cyber_essentials_0914.pdf

Cybersecurity Tech Accord. 2019. 'Cybersecurity Tech Accord – Protecting Users and Customers Everywhere'. As of 10 November: https://cybertechaccord.org/accord

EastWest Institute. 2016. *Purchasing Secure ICT Products and Services: A Buyers Guide*. As of 10 November 2019: https://www.eastwest.ngo/idea/purchasing-secure-ict-products-and-services-buyers-guide

European Commission (EC). 2019a. '5G Research & Standards'. As of 10 November 2019: https://ec.europa.eu/digital-single-market/en/research-standards

———. 2019b. 'Member States Publish a Report on EU Coordinated Risk Assessment of 5G Networks Security'. As of 10 November 2019: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

European Union Agency for Network and Information Security (ENISA). 2015. *Supply Chain Integrity – An Overview of the ICT Supply Chain Risks and Challenges, and Vision for the Way Forward.* Version 1.1. As of 10 November 2019: https://www.enisa.europa.eu/publications/sci-2015/at_download/fullReport

Exostar. 2019a. 'Risk Management'. As of 10 November: https://www.exostar.com/solution/risk-management

———. 2019b. 'Solutions'. As of 10 November: https://www.exostar.com/solutions

———. 2019c. 'What is CMMC?' As of 10 November: https://www.exostar.com/cmmc

France Diplomatie (Ministry for Europe and Foreign Affairs). 2018. *Paris Call for Trust and Security in Cyberspace*. As of 10 November 2019: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Global Commission on the Stability of Cyberspace (GCSC). 2018. *Norm Package Singapore*. As of 10 November 2019: https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf

Greenberg, Andy. 2018. 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'. Wired, 22 August, 5.00 a.m. As of 10 November 2019: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

Group of Seven/Eight (G7/8) Foreign Ministers Meetings. 2019. 'Dinard Declaration on the Cyber Norm Initiative'. G7 Information Centre. As of 10 November 2019: http://www.g7.utoronto.ca/foreign/190406-cyber.html

GSMA. 2019. 'Network Equipment Security Assurance Scheme (NESAS)'. As of 10 November 2019: https://www.gsma.com/security/network-equipment-security-assurance-scheme

Heinbockel, William J., Ellen R. Laderman & Gloria J. Serrao. 2017. *Supply Chain Attacks and Resiliency Mitigations – Guidance for System Security Engineers*. The MITRE Corporation. As of 10 November 2019: https://www.mitre.org/sites/default/files/pdf/PR_18-0854.pdf

Hober, Kaj. 2019. 'Report of Prof Dr Kaj Hober.' Kaspersky. As of 10 November 2019: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2015/02/02060120/REPORT-OF-PROF-DR-KAJ-HOBER.pdf

Huawei. 2019. 'Huawei Cyber Security Transparency Centre Opens in Brussels'. Huawei.com, 5 March. As of 10 November 2019: https://www.huawei.com/ch-en/press-events/news/2019/3/huawei-cyber-security-transparency-centre-brussels

Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. 2018. *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018 – A Report to the National Security Adviser of the United Kingdom*. UK Government. As of 10 November 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

———. 2019. *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019 – A Report to the National Security Adviser of the United Kingdom*. UK Government. As of 10 November 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

Information Security Policy Council. 2014. *The Basic Policy of Critical Information Infrastructure Protection (Tentative Translation).* 3rd ed. National Center of Incident Readiness and Strategy for Cybersecurity. As of 10 November 2019: https://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

International Organization for Standardization (ISO). 2006. *ISO/IEC 16085:2006. Systems and Software Engineering – Life Cycle Processes – Risk Management.* As of 10 November 2019: https://www.iso.org/standard/40723.html

———. 2007a. *ISO 28000:2007. Specification for Security Management Systems for the Supply Chain.* As of 10 November 2019: https://www.iso.org/standard/44641.html

———. 2007b. *ISO 28001:2007. Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments and Plans – Requirements and Guidance.* As of 10 November 2019: https://www.iso.org/standard/45654.html

———. 2011. *ISO/IEC 15026-2:2011. Systems and Software Engineering – Systems and Software Assurance – Part 2: Assurance Case.* As of 10 November 2019: https://www.iso.org/standard/52926.html

———. 2013. *ISO/IEC 27002:2013. Information Technology – Security Techniques – Code of Practice for Information Security Controls*. As of 10 November 2019: https://www.iso.org/standard/54533.html

———. 2014. *ISO/IEC 27036-1:2014. Information Technology – Security Techniques – Information Security for Supplier Relationships – Part 1: Overview and Concepts*. As of 10 November 2019: https://www.iso.org/standard/59648.html

———. 2015a. *ISO/IEC 20243:2015. Information Technology – Open Trusted Technology Provider Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products*. As of 10 November 2019: https://www.iso.org/standard/67394.html

———. 2015b. *ISO/IEC/IEEE 15288:2015. Systems and Software Engineering – System Life Cycle Processes.* As of 10 November 2019: https://www.iso.org/standard/63711.html

———. 2017. *ISO/IEC/IEEE 12207:2017. Systems and Software Engineering – Software Life Cycle Processes.* As of 10 November 2019: https://www.iso.org/standard/63712.html

———. 2018a. *ISO 31000:2018. Risk Management – Guidelines*. As of 10 November 2019: https://www.iso.org/iso-31000-risk-management.html

———. 2018b. *ISO/IEC 27005:2018. Information Technology – Security Techniques – Information Security Risk Management.* As of 10 November 2019: https://www.iso.org/standard/75281.html

———. 2018c. *ISO/IEC 27005:2018 — Information Technology — Security Techniques — Information Security Risk Management*. 3rd ed. As of 10 November 2019: https://www.iso.org/standard/75281.html

———. 2018d. *ISO/IEC 20243-1:2018. Information Technology – Open Trusted Technology Provider Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products – Part 1: Requirements and Recommendations.* As of 10 November 2019: https://www.iso.org/standard/74399.html

———. 2019. 'ISO/IEC 27001. Information Security Management'. As of 10 November: https://www.iso.org/isoiec-27001-information-security.html

Karygiannis, Tom, Bernard Eydt, Greg Barber, Lynn Bunn & Ted Phillips. 2007. *Guidelines for Securing Radio Frequency Identification (RFID) Systems – Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-98. Gaithersburg: National Institute of Standards and Technology. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-98.pdf

Kaspersky. 2019a. 'Kaspersky Receives SOC 2 Audit – Kaspersky Successfully Passes Independent SOC 2 Audit by One of the Big Four'. As of 10 November: https://www.kaspersky.com/about/compliance-soc2?ignoreredirects=true

———. 2019b. 'Operation ShadowHammer'. Kaspersky Securelist, 25 March, 1.01 p.m. As of 10 November: https://securelist.com/operation-shadowhammer/89992

———. 2019c. 'Transparency'. As of 10 November: https://www.kaspersky.com/about/transparency?ignoreredirects=true

Kavanagh, James. 2017. *Assuring the Security of Cloud Services*. Microsoft. As of 10 November 2019: http://download.microsoft.com/download/1/5/a/15abb577-bd3c-4cc4-9aa2-0ee1337714de/msft_safe_handbook.pdf

Lindberg, Randy. 2018. 'Using NIST Cybersecurity Framework to Assess Vendor Security'. Rivial Security, 10 April. As of 10 November 2019: https://www.rivialsecurity.com/blog/using-nist-cybersecurity-framework-to-assess-vendor-security

Martin, Ciaran. 2018. 'Letter to Permanent Secretaries Regarding the Issue of Supply Chain Risk in Cloud-Based Products'. National Cyber Security Centre, 15 November. As of 10 November 2019: https://www.ncsc.gov.uk/information/letter-permanent-secretaries-regarding-issue-supply-chain-risk-cloud-based-products

Microsoft. 2017. 'Securing the Supply Chain with Risk-Based Assessments'. Microsoft.com, 14 December. As of 10 November 2019: https://www.microsoft.com/en-us/itshowcase/securing-the-supply-chain-with-risk-based-assessments

———. 2018. ‘A Digital Geneva Convention to Protect Cyberspace’. Policy paper. As of 10 November 2019: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

Microsoft Defender ATP Research Team. 2018. ‘Attack Inception: Compromised Supply Chain within a Supply Chain Poses New Risks’. Microsoft Security Blog, 26 July. As of 10 November 2019: https://www.microsoft.com/security/blog/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks

Microsoft Security Intelligence. 2017. ‘Win32/Floxif’. Microsoft.com, 20 September. As of 10 November 2019: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Floxif

Ministry of Economy, Trade and Industry of Japan (METI). 2019. *The Cyber/Physical Security Framework (Draft).* As of 10 November: https://www.meti.go.jp/press/2018/01/20190109001/20190109001-4.pdf

National Cyber Security Centre (NCSC). 2017. ‘The 2017 Annual Review’. NCSC.gov.uk, 2 October. As of 10 November 2019: https://www.ncsc.gov.uk/news/2017-annual-review

———. 2018. ‘Supply Chain Security Guidance’. NCSC.gov.uk, 28 January. As of 10 November 2019: https://www.ncsc.gov.uk/collection/supply-chain-security

Nissen, Chris, John Gronager, Robert Metzger & Harvey Rishikof. 2019. *Deliver Uncompromised – A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War.* The MITRE Corporation. As of 10 November 2019: https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf

North American Electric Reliability Corporation (NERC). 2018. *CIP-013-1 – Cyber Security – Supply Chain Risk Management*. As of 10 November 2019: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf

North American Transmission Forum (NATF). 2018. *Cyber Security Supply Chain Risk Management Guidance.* Version 1.0. North American Electric Reliability Corporation. As of 10 November 2019: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf

Office of the Under Secretary of Defense for Acquisition and Sustainment. 2019. *Cybersecurity Maturity Model Certification (CMMC), Draft*. Version 0.6. As of 10 November 2019: https://www.acq.osd.mil/cmmc/docs/CMMC-V0.6b-20191107.pdf

Oldehoeft, Arthur E. 1992. *Foundations of a Security Policy for Use of the National Research and Educational Network*. NISTIR 4734. NIST Publications. doi:10.6028/NIST.IR.4734

Organization for Security and Co-operation in Europe (OSCE). 2016. *Decision No. 1202. OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.* OSCE Document PC.DEC/1202, 10 March. As of 10 November 2019: https://www.osce.org/pc/227281

Porter, Jon. 2019. ‘UK Watchdog Slams Huawei over “Serious” Cybersecurity Vulnerabilities’. The Verge, 28 March, 7.48 a.m. EDT. As of 10 November 2019: https://www.theverge.com/2019/3/28/18285185/huawei-uk-government-cybersecurity-report-5g-rollout-security-concerns

PricewaterhouseCoopers (PwC). 2019. ‘System and Organization Controls (SOC) Reporting’. As of 10 November: https://www.pwc.com/us/en/services/risk-assurance/third-party-assurance/soc-reporting.html

Purdy, Andy. 2016. *The Global Cyber Security Challenge – It is Time for Real Progress in Addressing Supply Chain Risks*. Huawei Technologies. As of 10 November 2019: https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/the-global-cyber-security-challenge-en.pdf

Robert H. Smith School of Business. 2015. *CyberChain – Guidelines to Measure and Assess Cyber Supply Chain Risks.* University of Maryland. As of 10 November 2019: https://cyberchain.rhsmith.umd.edu

SAE International. 2012. *AS6081. Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors.* As of 10 November 2019: https://www.sae.org/standards/content/as6081

———. 2019. ‘About SAE International’. As of 10 November: https://www.sae.org/about

SAFECode. 2009. *The Software Supply Chain Integrity Framework – Defining Risks and Responsibilities for Securing Software in the Global Supply Chain*. As of 10 November 2019: http://safecode.org/publication/SAFECode_Supply_Chain0709.pdf

———. 2019a. ‘Charter Members’. As of 10 November: https://safecode.org/members

———. 2019b. ‘Publications’. As of 10 November: https://safecode.org/publications

———. 2019c. ‘SAFECode Principles’. As of 10 November: https://safecode.org/safecode-principles

Security Scorecard. 2019. ‘SecurityScorecard – Supplier Risk Management Platform’. InfoGuard. As of 10 November: https://www.infoguard.ch/en/partners/security-scorecard-security-rating

SEMI. 2009. *SEMI T20 – Specification for Authentication of Semiconductors and Related Products*. As of 10 November 2019: https://store-us.semi.org/products/t02000-semi-t20-specification-for-authentication-of-semiconductors-and-related-products

———. 2014. *SEMI T21 – Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain.* As of 10 November 2019: https://store-us.semi.org/products/t02100-semi-t21-specification-for-organization-identification-by-digital-certificate-issued-from-certificate-service-body-csb-for-anti-counterfeiting-traceability-in-components-supply-chain

———. 2019. ‘About SEMI’. As of 10 November: https://www.semi.org/en/about

Siemens AG. 2019a. ‘Charter of Trust – Creating Trust in a Secure Digital World’. As of 10 November: https://new.siemens.com/kr/en/company/topic-areas/digitalization/cybersecurity.html

———. 2019b. ‘Charter of Trust: Shaping the future of security’. Atos. As of 10 November 2019: https://atos.net/wp-content/uploads/2019/06/CT_J2264_190509_RY_PP_THECHARTER_WEB_V3.pdf

———. 2019c. ‘Siemens Establishes Binding Cybersecurity Requirements for Suppliers’. Siemens.com/Press, 15 February. As of 10 November 2019: https://press.siemens.com/global/en/pressrelease/siemens-establishes-binding-cybersecurity-requirements-suppliers

Siemens, AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, Enel, IBM, MSC, NXP, SGS, Total & TÜV SÜD Munich. 2019. 'The Charter of Trust Takes a Major Step Forward to Advance Cybersecurity'. Siemens.com/Press, 15 February. As of 10 November 2019: https://press.siemens.com/global/en/pressrelease/charter-trust-takes-major-step-forward-advance-cybersecurity

Stockton, Paul. 2018. *Securing Critical Supply Chains: Strategic Opportunities for The Cyber Product International Certification (CPIC^{TM}) Commission Initiative*. EIS Council. As of 10 November 2019: https://www.eiscouncil.org/App_Data/Upload/8c063c7c-e500-42c3-a804-6da58df58b1c.pdf

Suffolk, John. 2013. *Cyber Security Perspectives – Making Cyber Security a Part of a Company's DNA – A Set of Integrated Processes, Policies and Standards*. White paper. Huawei Technologies. As of 10 November 2019: https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/hw-cyber-security-wp-2013-en.pdf

———. 2014. *Cybersecurity Perspectives – 100 Requirements When Considering End-to-End Cybersecurity with Your Technology Vendors.* Huawei Technologies. As of 10 November 2019: https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/hw-cyber-security-wp-2014-en.pdf

Sweney, Mark. 2019. 'Huawei Issues Could Pose UK Security Risks, Say Authorities'. *Guardian*, 28 March, 12.10 p.m. GMT. As of 10 November 2019: https://www.theguardian.com/technology/2019/mar/28/huawei-chinese-firm-poses-national-security-risks-says-uk-watchdog

The Open Group. 2015a. 'The Open Trusted Technology Provider™ Standard (O-TTPS) Approved as ISO/IEC International Standard'. The Open Group Blog, 2 September. As of 10 November 2019: https://blog.opengroup.org/2015/09/02/the-open-trusted-technology-provider-standard-o-ttps-approved-as-isoiec-international-standard

———. 2015b. *Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.1 (Identical to ISO/IEC 20243:2015)*. As of 10 November 2019: https://publications.opengroup.org/c147

———. 2017. *Open Trusted Technology Provider™ Standard (O-TTPS) – Certification Policy, Version 1.1.* As of 10 November 2019: https://ottps-cert.opengroup.org/sites/ottps-cert.opengroup.org/files/doc/O-TTPS_Certification_Policy.pdf

———. 2019. 'About Trusted Technology'. As of 10 November: https://www.opengroup.org/forum/trusted-technology-forum

Tikk, Eneken, & and Mika Kerttunen. 2018. *Parabasis – Cyber-diplomacy in Stalemate*. NUPI Report 5/2018. Norwegian Institute of International Affairs. As of 10 November 2019: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2569401/NUPI_Report_5_18_Tikk_Kerttunen.pdf

TrendLabs. 2017. *2017 Midyear Security Roundup: The Cost of Compromise*. Trend Micro. As of 10 November 2019: https://documents.trendmicro.com/assets/rpt/rpt-2017-midyear-security-roundup-the-cost-of-compromise.pdf

United Nations General Assembly (UNGA). 2013. *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, UN Document A/68/98, 24 June 2013. As of 10 November 2019: https://undocs.org/A/68/98

———. 2015a. 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. International code of conduct for information security', UN Document A/69/723, 13 January 2015. As of 10 November 2019: https://undocs.org/A/69/723

———. 2015b. *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, UN Document A/70/174, 22 July 2015. As of 10 November 2019: https://undocs.org/A/70/174

US Federal Energy Regulatory Commission (FERC). 2016. *Revised Critical Infrastructure Protection Reliability Standards*. Docket No. RM15-14-002, Order No. 829, 21 July. As of 10 November 2019: https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf

US National Institute of Standards and Technology (NIST). 2013. *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST Special Publication 800-53, Revision 4. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

———. 2015a. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* NIST Special Publication 800-161. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

———. 2015b. *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*. NISTIR 8074, Vol. 2. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

———. 2017. 'Software Supply Chain Attacks'. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf

———. 2018a. *Framework for Improving Critical Infrastructure Cybersecurity.* Version 1.1. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

———. 2018b. 'Cybersecurity Framework Usage'. As of 10 November 2019: https://www.nist.gov/industry-impacts/cybersecurity

———. 2018c. 'Information and Communications Technology Supply Chain Risk Management (ICT SCRM)'. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf

———. 2019a. 'Cyber Supply Chain Risk Management'. As of 10 November: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management

———. 2019b. 'Cyber Security Supply Chain Risk Management – Industry Best Practices for Cyber SCRM'. As of 10 November 2019: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/Best-Practices

VeraCode. 2019. 'Vendor Application Security Testing'. As of 10 November: https://www.veracode.com/security/vendor-application-security-testing

Zetter, Kim. 2019. 'Hackers Hijacked Asus Software Updates to Install Backdoors on Thousands of Computers'. MotherBoard, 25 March, 9.00 a.m. As of 10 November 2019: https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

40 UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH