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 & 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 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.

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

3GPP	3rd Generation Partnership Project
BSI	Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik)
CBM	Confidence-building measure
CEN	European Committee for Standardization (French: Comité Européen de normalisation)
CENELEC	European Committee for Electrotechnical Standardization (French: Comité Européen de normalisation électrotechnique)
CNSS	Committee on National Security Systems
CPNI	Centre for the Protection of National Infrastructure
C-SCRM	Cyber Supply Chain Risk Management
ETSI	European Telecommunications Standards Institute
G7	Group of Seven
GCSC	Global Commission on the Stability of Cyberspace
GGE	Group of Governmental Experts
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IGO	Intergovernmental Organization
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NCSC	National Cyber Security Centre

NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
OEWG	Open-ended Working Group
OSCE	Organization for Security and Co-operation in Europe
O-TTPS	Open Trusted Technology Provider Standard
SCO	Shanghai Cooperation Organisation
SCRM	Supply Chain Risk Management
SME(s)	Small and Medium Enterprise(s)
(T)CBMs	(Trust and) Confidence-building Measures
TSC(s)	Technology Supply Chain(s)
UNGA	United Nations General Assembly

EXECUTIVE SUMMARY

A supply chain is traditionally understood as a system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier (producer) to customer. Today, with the advent of global digital transformation, supply chains and the ways they are managed are transforming, with increasing risks and threats to their security and integrity. These trends highlight the increasing need for internationally shared, adoptable and scalable solutions that could reverse or tamp down cyber threats to supply chains through cooperative efforts of governments, industry, the technology community and other stakeholders.

Supply chain security is one of the key issues in multilateral norm development processes related to information and communications technology (ICT), and it continues to be a main point of discussion under two new multilateral cyber processes launched in 2018 under the auspices of the United Nations General Assembly: a new United Nations Group of Governmental Experts (GGE) and an Open-ended Working Group (OEWG) focused on developments in the field of ICT in the context of international security.

This report aims to assess how normative responses to ICT-related challenges to supply chain security could be further advanced and operationalized. As norms reflect shared expectations, or standards, of appropriate behaviour, identifying opportunities for improving their operationalization requires looking beyond norms themselves and contextualizing them in the wider ecosystem of responses to supply chain security challenges to identify gaps and areas for improvement.

EVOLVING DIGITAL THREAT LANDSCAPE FOR SUPPLY CHAINS

Increases in the scale of malicious cyber activities targeting supply chains have been reported by private enterprises, government agencies and cybersecurity experts across the world. More specifically, software supply chain attacks have become one of the key cyber threats to industry and other stakeholders as increased cybersecurity awareness and specific countermeasures have made more common cyberattacks less effective and more expensive.

Compromise of hardware and firmware components in supply chains has also become an increasing concern among governments, private enterprises and cybersecurity experts. This includes reports of tailored operations by malicious actors aimed at compromising supply chains through the insertion of hidden functions and software and hardware backdoors.

RESPONSES TO ICT-DRIVEN CHALLENGES TO SUPPLY CHAIN SECURITY AND INTEGRITY

The current ecosystem of responses to ICT-driven challenges to supply chains is based on five interconnected and mutually reinforcing pillars:

1. Technical standardization frameworks
2. National legislative and regulatory frameworks
3. Corporate supply chain security management and supply chain security assurance policies
4. Capacity-building tools and resources
5. Normative frameworks

Technical standards serve as 'the common language' used to communicate expected levels of performance for products and services and are among the core pillars for complex technology-based ecosystems, global supply chains being no exception.

National regulatory policies and frameworks complement the development and enforcement of technical standards, allowing governments to develop and implement more comprehensive, holistic and effective cyber supply chain risk management (C-SCRM) among public and private sector organizations.

Corporate practices and frameworks include extensive toolkits of requirements for vendors, elaborated procedures, guidelines and best practices aimed at minimizing and mitigating ICT-related risks in corporate supply chains.

Capacity-building tools and resources offer a range of options for stakeholders interested in assessing and improving current practices. Those options include (self)-assessment and auditing tools and services for C-SCRM, digital platform solutions for secure collaboration and information-sharing among technology vendors, volunteer C-SCRM frameworks, and methods developed by industry and the technology community to help organizations manage their supply chain risks.

NORM-DEVELOPING FRAMEWORKS AND INITIATIVES

Within the supply chain security response ecosystem, norms represent the highest level, often serving as conceptual frameworks for more operational elements (e.g. standards, policies, regulations, guidelines). Norm-developing initiatives to address ICT-driven challenges to supply chain security and integrity can be broken down into three categories:

1. The United Nations-led multilateral processes – the current cyber GGE and the OEWG – both of which build on the 2015 GGE report and the set of norms included in it.
2. Initiatives of regional or other intergovernmental organizations also addressing supply chain issues in the context of ICT security and international cooperation (e.g. the Shanghai Cooperation Organisation, the Group of 7).
3. Multi-stakeholder norm-building initiatives by an expanding set of 'norm entrepreneurs' (e.g. the Cybersecurity Tech Accord, the Global Commission on the Stability of Cyberspace).

From a comparative analysis of different initiatives, the following observations can be made:

1. The total number of normative frameworks addressing the issue of supply chain security and integrity has rapidly increased over the last seven years – from, effectively, only the GGE in 2013 to eight initiatives in 2019.
2. Many of these frameworks (five out of eight) are multi-stakeholder frameworks developed and led either by technology industry actors (e.g. Microsoft, Siemens) or by mixed stakeholder groups including both States and technology sector actors (e.g. the Paris Call for Trust and Security in Cyberspace).
3. Regional organizations appear to be the most underrepresented type of actor addressing ICT supply chain security and integrity issues from a normative perspective.

4. Most (five) of the proposed norms are 'positive' ones, encouraging or binding States and other actors to take particular actions to mitigate ICT-driven threats to supply chain security and integrity. Two norms are 'negative', and one is mixed, combining 'positive' and 'negative' elements.

SUPPLY CHAIN SECURITY NORMATIVE GAPS AND RECOMMENDED MITIGATION ACTIONS

This study presents an initial mapping of 'gaps' in the proposed or emerging normative frameworks. In this context, gaps and limitations are not regarded as 'deficiencies', but rather as areas in which further elaboration on a normative initiative (or on courses of action supporting it) might contribute to advancement in its operationalization.

A set of possible recommendations has been designed to address such gaps and limitations, with the purpose of sparking discussion among policymakers, diplomats and other national experts involved in norm-building efforts, as well as among industry, the wider technology community and other stakeholder groups.

The gaps, limitations and related recommendations are summarized in the table below and further elaborated in the report.

GAPS, LIMITATIONS, AND RECOMMENDATIONS

GAPS & LIMITATIONS

1

Lack of observation incentives and implementation mechanisms for 'negative' norms

Such norm initiatives are challenged by lack of proper motivation and incentives for compliance among the actors they are targeting. The potential for effective observation of negative norms is limited by the well-known challenge of ensuring credible attribution of malicious cyber activities.

2

'Patchwork' nature of initiatives focusing on harmful hidden functions

Norms with a scope limited to backdoors set the hidden function risks apart from the rest of the ICT-driven risks to supply chains, and in doing so they break the paradigm of an integrated and comprehensive risk management approach.

RECOMMENDATIONS

Align the scope of proposed norms with a comprehensive SCRM approach and industry practices

Leveraging the mandate of the OEWG to further develop norms, rules and principles – specific actions could include:

- Ensuring a better balance between 'negative' and 'positive' norms
- Expanding the focus of (new or adopted) norms to address the whole continuum of ICT-driven risks and aligning the substance of proposed norms with approaches used by industry and the technology community

GAPS & LIMITATIONS

3

Overlaps and duplication of efforts by multi-stakeholder initiatives

While diversity of frameworks and initiatives, and even certain competition among them, boosts the global cybersecurity norm-building agenda, it could also result in dispersion of efforts. In particular, this trend generates the risk of multiple parallel SCRM frameworks competing for the status of de facto global standardized practice.

RECOMMENDATIONS

Strengthen coordination and synergy among multi-stakeholder norm-building initiatives and promote unified and interoperable minimum requirements for technology suppliers

Specific actions could include:

- Exploring opportunities to create structured and systematic communication flow and information-sharing among multi-stakeholder norm-building processes addressing global supply chain issues in the ICT context
- Launching a process for discussion and elaboration of a unified, or at least harmonized and interoperable, set of minimum security and certification requirements shared, supported and promoted jointly by major multi-stakeholder forums

GAPS & LIMITATIONS

4

Lack of standardized process frameworks for dealing with global technology vendors in national markets

Given the lack of international standards to ensure supply chain security when dealing with foreign technology providers, an increasing number of Member States are creating rules and requirements at the national level. This could result both in compromising the coherence (and effectiveness) of effort at the international level and in increasing compliance costs for vendors.

RECOMMENDATIONS

Harmonize national processes to work with transnational technology vendors

Explore the opportunities for coordination and harmonization across States of approaches and processes for the management of transnational technology vendors to make them more transparent and aligned with global SCRM and vendor security assessment standards.

GAPS & LIMITATIONS

5

Lack of coordination and synergy between intergovernmental normative initiatives, global industry and the technology community

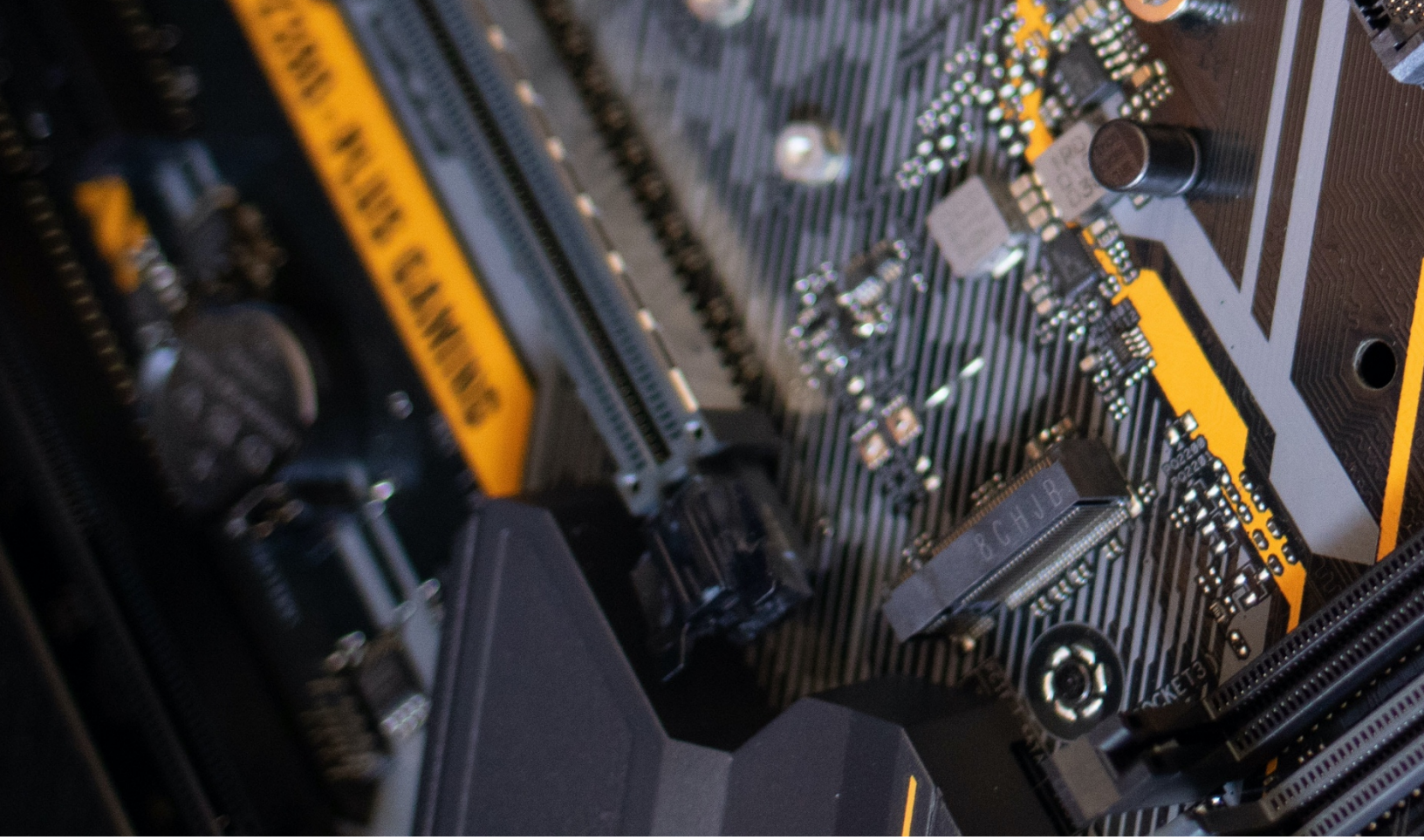
Norm-building efforts led by different actors (e.g. United Nations, industry, multi-stakeholder groups) all present different levels of maturity, different thematic emphasis and different representations. As these efforts are not a deliberate pursuit of complementary or supplementary processes, the impact of the overall set of initiatives appears suboptimal.

RECOMMENDATIONS

Consider establishing a dedicated platform to support United Nations-led processes in engaging with industry, the technology community and other multi-stakeholder groups and initiatives active in the supply chain security and integrity field

Within the mandate of the OEWG to establish regular institutional dialogue with broad participation, including of the private sector, consider establishing a dedicated platform (e.g. committee, task force) to support the operationalization of the international cybersecurity norms related to the integrity and security of supply chains.

The proposed platform is not intended to counterbalance or substitute the intergovernmental cyber norm-developing processes, but rather provide necessary support to them in areas in which the private sector has an inherent primary role in the implementation of proposed norms.



GAPS & LIMITATIONS

6

Lack of focus on addressing supply chain ICT-driven risks through capacity-building

Considering that the ecosystem of technology suppliers is globally dispersed, and many suppliers are based in jurisdictions lacking mature regulatory policies and standardization frameworks, international capacity-building efforts could considerably improve the overall risk environment in global supply chains.

RECOMMENDATIONS

Increase focus on capacity-building efforts

States should conduct, independently or with external support, a national capability assessment to identify gaps and capacity-building needs related to the mitigation of ICT risks to supply chains.

Regional organizations should do a similar exercise and should provide data, information and wider resources to support both States and technology vendors willing to do business in specific regions or countries.

Multilateral capacity-building initiatives should be developed to focus specifically on supply chain risks.

GAPS & LIMITATIONS

7

Lack of focus on using confidence-building measure (CBM) toolkits to address supply chain ICT-driven risks

Like capacity-building, the role that trust and confidence-building measures (TCBMs) could play in addressing ICT-driven risks to technology supply chains (TSCs) has been underexplored. Relative success in the adoption of CBMs at the regional level (Organization for Security and Co-operation in Europe in 2012 and 2016) and the bilateral level (US–Russian agreements of 2013) to mitigate transnational ICT-driven risks gives reason to further explore the adaptation of the CBM toolkit to managing cybersecurity challenges for TSCs.

RECOMMENDATIONS

Assess and identify opportunities for using the (T)CBM toolkit to ensure the security and integrity of TSCs

As part of the OEWG workings, investigate the need to expand the list of adopted cybersecurity (T)CBMs with measures specifically addressing the mitigation of cyber risks to TSCs or the need to formulate a contextual interpretation of already adopted (T)CBMs to reflect supply chain-specific issues. In addition, States should consider unilateral voluntary sharing of information on ICT-driven threats as well as reinforcing bilateral trust and transparency measures specifically targeting supply chain security and integrity.

GAPS & LIMITATIONS

8

Overall low level of maturity of national frameworks and initiatives to ensure security and integrity of TSCs at a national level

The majority of state-of-the-art responses at the national level to address ICT-driven risks to TSCs are concentrated within a limited number of States. The remaining picture demonstrates a much lower level of maturity in strategic, policy and regulatory responses to such challenges.

RECOMMENDATIONS

Strengthen the institutional, strategic and policy coordination of efforts to address ICT-driven challenges to TSCs at a national level

This recommendation has national scope and focuses on the need for improved (internal) coordination of States' efforts to mitigate ICT-driven challenges to supply chains at a domestic level.


COM-B
LINE-O
VID-O

INTRODUCTION

1.1 CONTEXT

Moving a product or a service from supplier to consumer often involves a system of organizations, people, technology, information and activities commonly referred to as a 'supply chain'.[1]

Cyber-related challenges to the integrity and security of global supply chains have been a focus of international norm-developing initiatives for several years. In this report, in accordance with the study by the World Bank, global norms are understood to be "the shared expectations or standards of appropriate behaviour accepted by States and intergovernmental organizations that can be applied to States, intergovernmental organizations, and/or [non-State] actors of various kinds". [2]

At the United Nations General Assembly (UNGA) level, norms focused on information and communications technology (ICT) and supply chains were explicitly addressed for the first time in the 2013 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (by the United Nations Group of Governmental Experts (GGE) on cybersecurity). The report identified risks to "secure and reliable ICT use and the ICT supply chain for products and services", making special focus on embedded hidden functions (so-called 'backdoors').[3] The GGE 2013 report also called on States to encourage the private sector and civil society to play an appropriate role in improving the security of ICTs, including supply chain security.[4] This recommendation was reiterated and expanded in the 2015 report of the subsequent (fourth) GGE among other proposed norms, rules and principles for the responsible behaviour of States.

Over last several years, however, the norm-developing efforts aimed at strengthening cybersecurity and the global stability of cyberspace have received major contributions from multi-stakeholder and private sector frameworks. Those include a range of initiatives led by major technology corporations, such as the Digital Geneva Convention to protect cyberspace by Microsoft or Siemens' cybersecurity Charter of Trust, and government-initiated multi-stakeholder efforts such as the Paris Call for Trust and Security in Cyberspace. These actors from the private industry, civil society and technology

1 For additional definitions, please refer to ENISA (2015); ISO (2014, part I).
2 Martinsson (2011).
3 UNGA (2013).
4 UNGA (2013).

communities, sometimes described as 'norm entrepreneurs',[5] have joined governmental and intergovernmental actors in the debate on cybersecurity norms and contributed to it a broad set of initiatives and efforts to develop and globally promote new mandatory requirements to supply chain security, integrity and transparency, as well as codified best practices, standards and certification benchmarks.

In this context, the fact that most proposed norms and recommendations developed by cyber norm entrepreneurs focus on the security and integrity of supply chains illustrates the relevance of ICT-driven challenges. This focus is also the result of the increasing costs from attacks and other malicious cyber activities affecting the security and integrity of global supply chains faced by the private sector.[6]

Large public entities and government organizations, especially in the defence sector, constitute a considerable share of the global technology buyers' market,[7] and as such they rely on ICT components, products and services, including commercial off-the-shelf products, supplied to them by private companies. This predetermines private industry's role as the first line of defence against threats to the security and integrity of global supply chains stemming from malicious use of ICTs, including software attacks and other types of hardware and software exploitation.

Today, playing this role is becoming increasingly difficult. Security experts report a rapid upsurge in the exploitation of technology supply chains (TSCs) as a preferred and common vector for cyberattacks, technology espionage and other activities conducted by a variety of actors, from cyber criminals to alleged State proxies. In addition, an increasing number of States have expressed concerns over the dependency of their industries and government agencies on foreign technology vendors in sensitive and critical sectors such as dual-use and defence technologies, and strategic digital technologies such as 5G communications.[8]

For international norm-developing processes, these trends furthermore highlight the need to ensure that norms (and supporting instruments, such as technical tools and best practices) are effectively operationalized to improve risk management and increase resilience against ICT-related threats to TSCs.

For the United Nations and its Member States, the window of opportunity for advancing in this direction is open now, with two parallel processes launched to address global

5 Hurel & Lobato (2018).
6 CrowdStrike (2018).
7 Evermann (2014).
8 EC (2019a); Feinstein (2019); US White House (2019b); Wright (2019).

cybersecurity challenges: the sixth GGE and a new Open-ended Working Group (OEWG), established through UNGA resolution A/RES/73/27 in late 2018.[9]

1.2 SCOPE AND PURPOSE OF THE REPORT

This report aims to assess how normative responses to ICT-related challenges to supply chain security could be further advanced and operationalized.

This report is intended to support policy and decision makers engaged in multilateral, regional and national processes related to cyber norm-development. In addition, this report could benefit other stakeholder groups, such as private sector companies, civil society and technology communities.

1.3 STRUCTURE OF THE REPORT

This report is organized into several thematic blocks. In particular:

- *Chapter 2* provides an overview of key current digital technology-related trends impacting global supply chains, including the convergence of physical and digital supply chains, the proliferation of cybersecurity risks in supply chain relationships, and other relevant trends.
- *Chapter 3* provides a basic overview of ICT-driven challenges, risks and threats to the security and integrity of supply chains across different sectors and jurisdictions. This includes a basic classification of cybersecurity risks to supply chains, as well as an overview of selected cybersecurity incidents and attacks affecting supply chains in recent years.
- *Chapter 4* provides an overview of the ecosystem of responses to ICT-driven challenges affecting supply chains, including technical standardization, national legal and regulatory frameworks, corporate practices, and capacity-building initiatives.
- *Chapter 5* explores the global normative initiatives focused on ensuring the security and integrity of supply chains in the context of ICT-driven challenges, including the GGE norms and other normative frameworks.
- *Chapter 6* identifies and explores gaps between the normative mechanisms and initiatives, and practical (technical and organizational) mechanisms and instruments developed and currently used by industry actors and other stakeholders to ensure security, integrity and transparency in their supply chains.

9 UNGA (2018).

- *Chapter 7*, building on this gap analysis, identifies recommendations for multilateral, regional and national interventions to strengthen supply chain security and integrity in the context of ICT-driven challenges.

Given the technical nature of the subject of this report, a separate document titled 'Technical Compendium' includes additional supporting information presented in eight technical annexes, covering information such as:

- Standardized definitions of key terms related to supply chain security and integrity (Annex I)
- Selected cases of supply chain attacks (Annex II)
- Standardization frameworks addressing supply chain security and integrity in the context of ICT-driven risks and threats (Annex III and Annex IV)
- Overview of governmental and industry-led guidelines and non-standardized best practices for managing ICT-driven risks to supply chains (Annex V)
- Selected cases of corporate SCRM and security assurance frameworks (Annex VI)
- (Self-)assessment and auditing tools for supply chain cyber risk management (Annex VII)
- Summary of international and multi-stakeholder normative initiatives addressing ICT supply chain security and integrity (Annex VIII)

TECHNOLOGY TRENDS ACROSS GLOBAL SUPPLY CHAINS

2.1 SUPPLY CHAINS IN THE AGE OF DIGITAL TRANSFORMATION

ICT – or digital technologies – play an increasingly dominant role in the organization and operation of global supply chains, as well as in localized supply chains of commercial enterprises and government organizations. Therefore, the security and integrity of the supply chain for ICT products and services is relevant across multiple sectors. The reason is that the global digital transformation of industries and sectors of the economy, which makes the ICT component omnipresent and cross-sectoral, also triggers the global transformation of supply chain security management and relationships between suppliers and acquirers. While global supply chains for ICTs themselves (e.g. supply chains of software and hardware components for ICT products and services) are at the forefront of technology developments, the ICT-driven challenges to supply chain security and integrity nowadays span far beyond the ICT sector and are cross-cutting in nature.

The increasing global dependency of supply chains on ICTs has several 'brand names'. The World Trade Organization describes it as 'Supply Chain 4.0': the reorganization of supply chains (design and planning, production, distribution, consumption, and reverse logistics) using technologies that are known as 'Industry 4.0'.[10] The birth of this now-global trend took place among large commercial enterprises in the technology sectors of high-income

10 World Bank & WTO (2019).

countries in an effort to increase the efficiency of supply chain management through the use of innovative digital technologies (e.g. cloud computing, artificial intelligence, distributed ledgers).

Further, the advent of 5G, the Internet of Things (IoT) and the Industrial IoT, as well as the digitalization of 'vertical industries', is expected to increase the penetration of ICTs to the very core of business and technological processes throughout multiple sectors, further deepening the dependency on ICTs across them. As stated by Michael Spence, Nobel Laureate in Economics: "One clear message is that as economies move to being built in part on digital foundations, trade, [global value chains] and digital technology cannot be separated and dealt with as independent trends and forces."[11]

One insightful reflection on this transformation is provided by the Ministry of Economy, Trade and Industry of Japan in its draft Cyber/Physical Security Framework, released in 2017.[12] The document stresses increasing convergence between cyberspace and the physical domain through digital technologies, including cyber–physical systems and interfaces, and the accompanying transformation of the very nature of supplier–client relationships and interactions.

In contrast with the traditional linear supply chain model, with the advent of digital technologies and ICT-enabled business processes across industries and sectors, a new structure and logic has emerged in the global supply chain. This new supply chain paradigm (which, in addition to being referred to as Supply Chain 4.0, is described as the 'Society 5.0 supply chain'[13]) is based on the following characteristics:

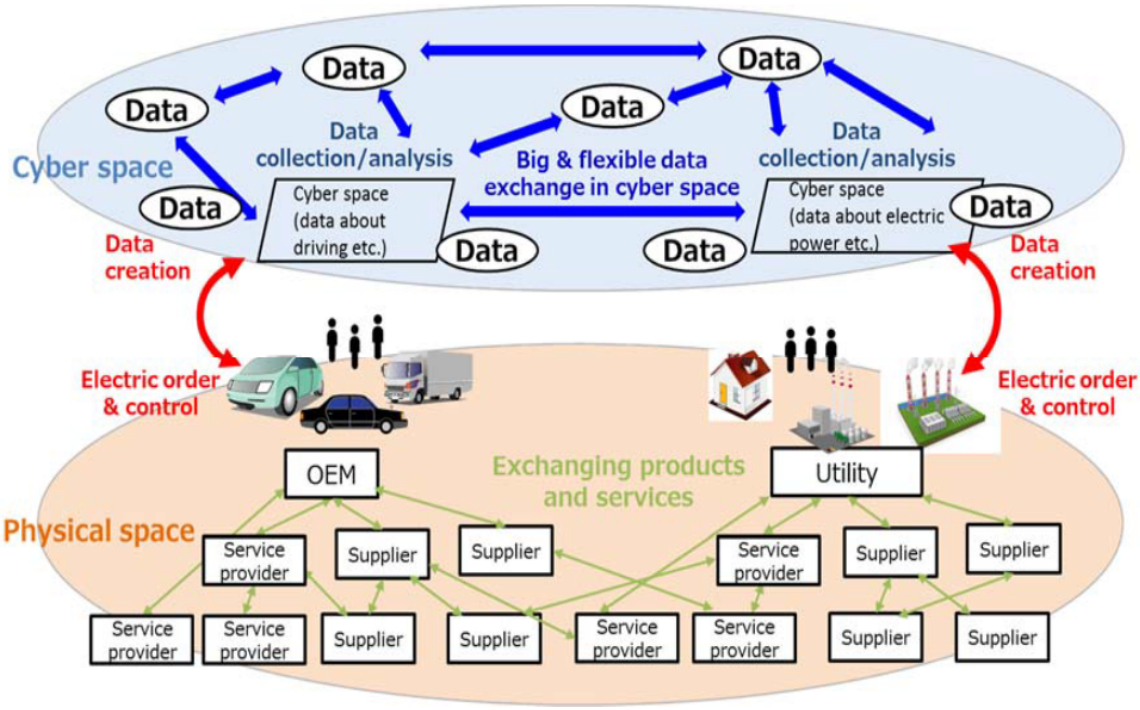
- *Deep convergence and integration of offline and online processes throughout the supply chain life cycle*: Digital technologies become inherent and irreplaceable for the supply chain itself and for its management, including continuous monitoring of supply chain integrity and risks via data-driven processes.
- *On-demand logic*: Items and services are provided to people who need them when they need them; the supply chain processes become increasingly customer-driven.
- *Flexibility*: The starting point of a series of activities to create added value is not fixed.
- *Data-driven management and decision-making*: Supply chain processes and activities may change during their life cycle if new solutions, approaches or requests are identified in the analysis of collected digital data.

11 World Bank & WTO (2019).
12 METI (2019a).
13 See: METI (2019a).

- *Decomposition of hierarchy*: Blending of operational and information technologies and infrastructures, increasingly flexible and customer-driven relationships in the market, and better data-driven awareness of managers make rigid hierarchy unnecessary for decision-making in supply chain management and relationships with vendors and customers. Instead of a linear model in which instructions flow along the chain, 'supplier–producer–distributor–consumer' and back, Supply Chain 4.0 introduces an integrated model in which the information flow has multiple directions.[14]

A schematic overview of this new Supply Chain 4.0 and the connections between multiple suppliers, other entities dependent on the supply chain, and digital data flows are represented in Figure 2.1.

Figure 2.1 - Connections between suppliers, other entities, and digital data flows in Supply Chain 4.0



OEM = Original equipment manufacturer Source: METI (2019a, 2)

14 See: METI (2019a, 2–4).

2.2 CHARACTERISTICS OF SUPPLY CHAIN 4.0

The emergence of Supply Chain 4.0 – or the Society 5.0 supply chain – has been gaining critical momentum across multiple sectors, jurisdictions and regions. According to market studies covering companies from across regions and sectors, 33 per cent of enterprises have already achieved high-level digitalization in their supply chain management, and an increase to 72 per cent is expected by 2021.[15]

In this context, it is possible to observe four high-level and cross-sector trends, which could have controversial implications in terms of supply chain security, resiliency and transparency, as well as SCRM:

- Increased complexity and globalization
- Increased cross-border interdependency
- Increased digitized management of supply chains
- Expanding security implications

Each of these trends is briefly discussed below.

2.2.1 COMPLEXITY AND GLOBALIZATION

Supply chains with a major ICT component are becoming increasingly globalized and complex. While this trend has been mentioned in many studies and reports,[16] its scale is probably best illustrated by the scale and structural complexity of the supply chains of major technology corporations:

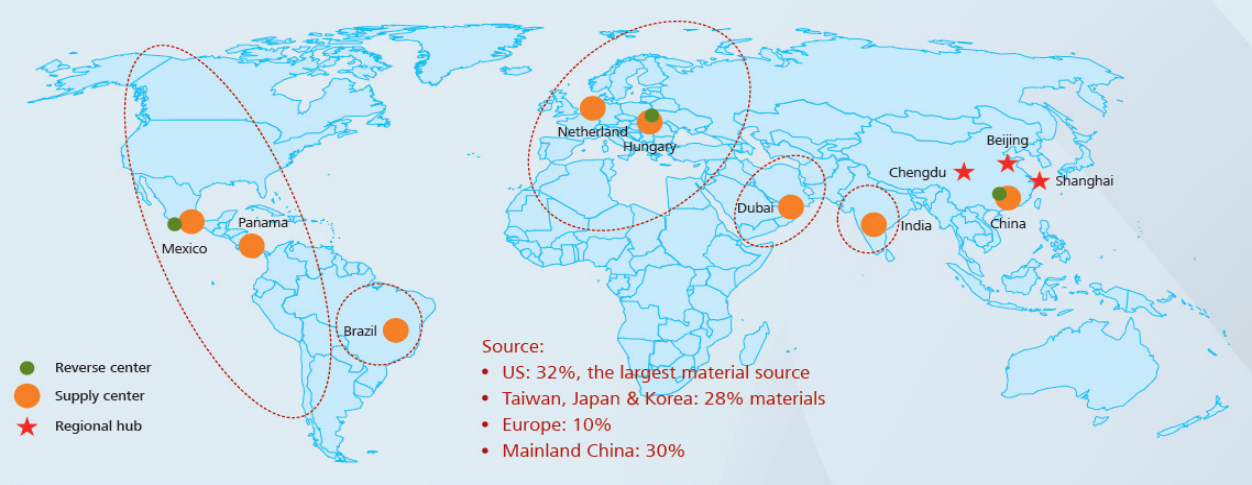
- The Apple Supplier List as of 2018 incudes 200 suppliers from over a dozen jurisdictions, which is not an exhaustive list.[17]
- Samsung's supply chain operates with over 2,000 suppliers across the globe.[18]
- Google works with more than 500 active suppliers in over 60 countries that provide hardware for the company's consumer devices and data centres, as well as services to support Google operations.[19]
- Huawei's list of suppliers, which combined represent 90 per cent of the company's procurement spending, included 1,183 vendors from multiple countries as of 2018.[20]

15 PwC (2016, 11).
16 Khan (2018); ResearchMoz (2019); World Bank & WTO (2019).
17 Apple Inc. (2019).
18 Samsung (2019).
19 Google (2018).
20 Huawei (2019).

- As of 2017, IBM's global supply chain operated with 13,000 first-tier suppliers in more than 100 countries.[21]

A visual representation of the complexity and transcontinental nature of a global TSC, in this case related to Huawei, is provided in Figure 2.2.

Figure 2.2 - Huawei global supply chain (as of June 2016)



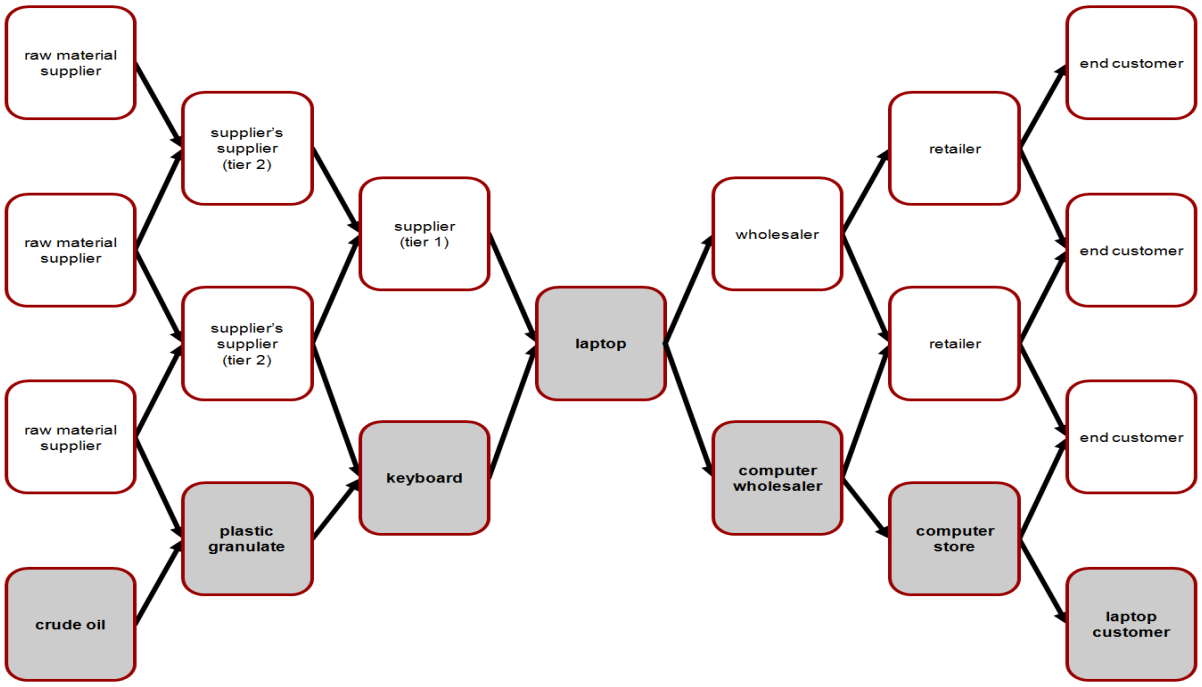
Source: Purdy (2016)

Apart from the global scale and geographic diversity, the high number of suppliers also contributes to the structural complexity of the supply chains of major enterprises and large public organizations (e.g. the US Department of Defense supply chain is estimated to operate with over 100,000 direct suppliers and many more indirect).[22] First and foremost, this complexity is due to the nested nature of supply chains: suppliers providing components, products or services to an organization have their own supply chains, network of connections and supplier–acquirer relationships with other vendors. From the standpoint of an organization, its immediate vendors are its so-called 'tier 1 vendors', and those who supply products and services to its 'tier 1 vendors' are 'tier 2 vendors'. For larger entities, which may have thousands of entities in their supplier network, effective traceability of components in the supply chain becomes critically important for prompt cyber vulnerability management.

This networked ecosystem is schematically represented in Figure 2.3.

21 IBM (2017a).
22 Defense Business Board (2017).

Figure 2.3 - Multi-tier supply chain concept



Source: Wieland & Wallenburg (2011)

One major concern among security experts and government regulators has been the inability to effectively map and trace the complete supply chain beyond tier 1 vendors, although industry and regulators have taken some initiatives to directly address this issue.[23,24] For example, according to a 2016 report by the US National Institute of Standards and Technology (NIST), 72 per cent of companies in the United States did not have full visibility of their supply chain, and 50 per cent did not have a process for assessing the cybersecurity of their third-party providers.[25] For certain groups of suppliers (e.g. national defence and security bodies' contractors), these figures might be different owing to additional requirements and compliance procedures enforced by their acquirers.[26]

However, the lack of visibility throughout organizations' supply chains has been considered a principal challenge to SCRM in both private and public sectors.[27] Once a tainted or tampered product or component enters the upstream supply chain, it can compromise the supply chains of customer organizations in any tier. Thus, an organization

23 Office of the Under Secretary of Defense for Acquisition and Sustainment & Office of the Deputy Assistant Secretary of Defense for Industrial Policy (2018).
24 Parliamentary Office of Science and Technology (2017).
25 Weatherford (2018, 24).
26 Office of the Under Secretary of Defense for Acquisition and Sustainment (2019).
27 Joint Committee on the National Security Strategy (2018, 33).

needs to consider security risks throughout this complex multi-tier supply chain ecosystem, and this is why special attention has been paid to enforcing mandatory requirements for tier 1 vendors to leverage security assurances when dealing with their own suppliers.

2.2.2 CROSS-BORDER INTERDEPENDENCY

The digitalization and ongoing globalization of supply chains have made actors from different jurisdictions and regions increasingly connected and interdependent in terms of supplier–acquirer relationships. This trend is probably best illustrated by the common practice of software development outsourcing: even small and medium enterprises (SMEs) across the world hire third-party organizations or programmers to develop software.[28] In many cases, these third-party suppliers of software development services are be based in a different jurisdiction or a different region; for example, India and, more recently, South-East Asian and Latin American countries have become known as global software outsourcing factories for companies from the United States and other North-East Eurasian and Western European countries.[29]

The increased reliance of global technology companies on foreign suppliers has, in some cases, sparked security concerns ranging from cybersecurity to national security. Some of the most notable examples have been identified in reviews and assessments of risks associated with defence sector transborder supply chains. In the United States, a recent assessment of US defence industrial base and supply chain integrity identified a surprising level of dependency on foreign suppliers, including for some sensitive defence technologies, such as the manufacturing of printed circuit boards for defence sector needs.[30] Similar concerns were shared and assessments conducted by other governments, revealing a trend in which transborder TSC interdependency becomes considered a strategic risk.[31]

2.2.3 DIGITIZED MANAGEMENT OF SUPPLY CHAINS

Digital transformation has made its path to supply chain management even in markets and industries where the organization's supply chain itself does not include ICT components such as software or hardware. The whole new niche of digital supply chain management and the concept of 'digital supply chain' have emerged over the last decade. The global supply chain management software market has been rapidly growing and is

28 Computaris (2016); PwC (2015).
29 Designveloper (2019); BairesDev (2019).
30 Office of the Under Secretary of Defense for Acquisition and Sustainment & Office of the Deputy Assistant Secretary of Defense for Industrial Policy (2018).
31 CISA (2019); EC (2019d).

expected to reach $22.7 billion by 2024.[32] This market segment, driven by IT industry majors like IBM, Oracle, SAP and Vanguard Software, includes a range of services based on emerging digital technologies and aimed at increasing efficiency and flexibility in supply chain management:[33]

- Automated and digitalized communications, document flow and transactions with suppliers and acquirers with the help of business-to-business digital platforms and services.
- Supply chain management and decision-making support with the help of machine learning and artificial intelligence-based predictive analytics.
- End-to-end visibility of organizations' supply chains – from manufacturing sites to logistics and delivery networks – through data aggregation, analysis and visualization.
- Cloud-based services and cloud platforms intended to enable access to digital supply chain management ecosystems for smaller organizations with limited ICT resources. Such solutions may include cloud-based access to powerful cognitive computing platforms, such as IBM Watson.
- Automated warehouse and inventory management as a component of logistics management in the supply chain: applicable technologies range from IoT-based services enabling real-time tracking and data analytics of warehouses' utilized capacity to 3D printing of warehouse equipment.
- SCRM solutions to address challenges, including those based on big data aggregation, processing and analytics.

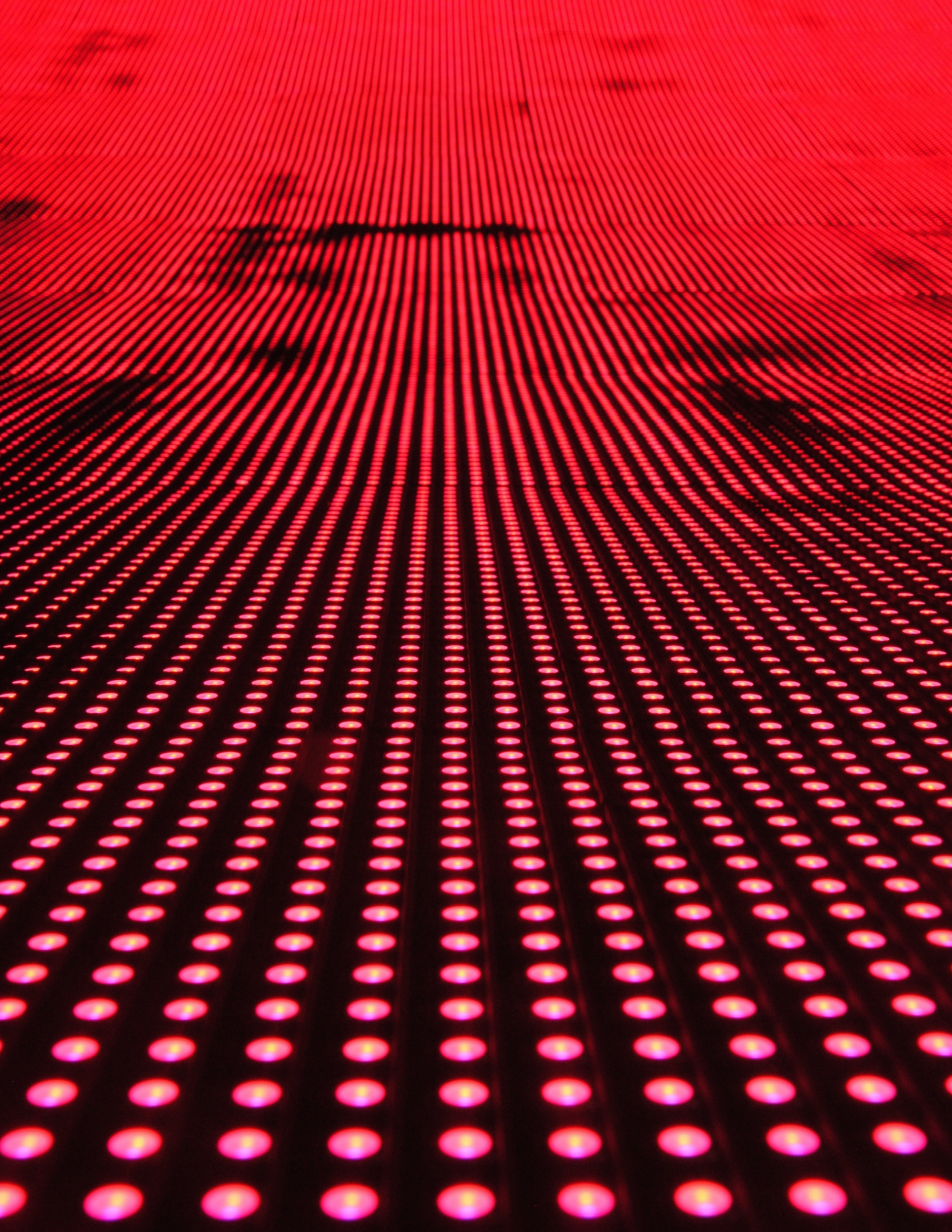
The paradox is that while these technology developments bring immense benefits by providing organizations with a powerful means to increase the efficiency of their supply chain operation, they also generate new cybersecurity risks for organizations.

2.2.4 SECURITY IMPLICATIONS

The cumulative effect of these developments is the unprecedented proliferation of cybersecurity risks across global TSCs and their participants. Expanded attack surface,[34] new entry points for malicious actors, and risk of disruption of technological processes and operations come to organizations as a reverse side effect of Supply Chain 4.0. While commercial enterprises and public organizations in general highlight the benefits of the global TSC ecosystem, not all have the capacity to face and mitigate these risks or are

32 PRNewswire (2018).
33 Bhargava et al. (2019); IBM (2017b); McKinsey & Company (2016); ResearchMoz (2019); SAP (2019).
34 Howard et al. (2003); Newman (2017).

even aware of them. The taxonomy and characteristics of cyber threats involving exploitation of TSCs are explained in more detail in the next chapter.



SUPPLY CHAIN DIGITAL THREAT LANDSCAPE

3.1 DYNAMICS OF ICT-DRIVEN ATTACKS AGAINST SUPPLY CHAINS

Technology trends transforming global ICT supply chains inevitably impact their security and integrity, as well as their global risk and threat landscape. The increasing complexity and multi-tiered nature of digitalized supply chains, the blurring of borders between information and operation processes and corresponding vendor relationships, and the proliferation of IoT and cyber–physical systems bring new challenges to TSC security management. Key evidence of this is the permanently increasing number and scale of security incidents targeting TSCs reported by private enterprises, government agencies and cybersecurity experts across the world. For example, industry studies and reports on supply chain cyberattacks over the last 3 years include the following:

- Symantec reported a 78 per cent increase in supply chain attacks in 2018.[35]
- Microsoft in its recent security intelligence report identified software supply chain attacks as one of the key threat vectors for industry and other stakeholders, stressing that the increased number of software supply chain attacks over the past few years has become one of the primary concerns in the technology industry and security community.[36] Finally, the publication points out the proliferation of supply chain attacks to the cloud as a particular concern, as they expand the scope of such malicious activities beyond software into cloud-based processes, services and infrastructures.[37]
- The US-based cybersecurity company CrowdStrike commissioned a global survey in 2019 which identified that 66 per cent of respondents had experienced some form of supply chain attack against their organization; 45 per cent of such security incidents had taken place in the preceding 12 months.[38]
- The ongoing increase in the number of supply chain cyberattacks and the proliferation of this threat vector, mostly in the software supply chain segment, as well as the mounting frequency and complexity of such attacks, were also mentioned among key cyber threat trends and expectations for 2019 by a number of cybersecurity companies, including Check Point, Cisco and Kaspersky.[39]

35 Symantec (2019).
36 Microsoft (2018b).
37 Microsoft (2018b).
38 Bourne (2018); CrowdStrike (2018).
39 Check Point Research (2019); Cisco (2018); Kaspersky (2019).

- Government agencies have also expressed concern over mounting risks to users and organizations posed by the growing number of high-profile ICT supply chains attacks. According to the US NIST Computer Security Resource Center, software supply chain attacks have become "an efficient way to bypass traditional defenses and compromise a large number of computers". In 2017, at least seven high-profile incidents were reported, compared with four such incidents over 2014–2016.[40]
- The US NIST mentions at least two reasons for the expected rise in software supply chain attacks:
  - The lack of proper cyber and process protections throughout the development and distribution channels of software vendors.
  - The increased cybersecurity awareness, maturity and strengthened cybersecurity posture of organizations' networks, components and computers, which has made other common attack vectors and techniques less effective or more expensive and difficult to execute.[41] This echoes opinions shared by major private companies; for example, according to Microsoft, a wave of software supply chain attacks taking advantage of vulnerabilities in software update tools could be due to better protection of modern digital platforms and operating systems as well as the decay of traditional infection vectors like browser exploits.[42]

Since 2017, the global upsurge in ICT supply chain attacks has taken place mostly across software supply chains. Some significant incidents of this type that have been reported in recent years are described in Annex II of the Technical Compendium.

An additional factor to consider is that some of the malicious cyber activities targeting supply chains may be covert and not revealed for a considerable period of time. One example of such malicious cyber activity is the insertion of hidden functionality into products or components in the supply chain that can be triggered remotely at a time and in a manner of the choosing of the malicious actors. These so-called 'logic bombs' are one particular type of hidden functionality, defined as "piece[s] of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met".[43]

40 US NIST-CSRC (2017).
41 US NIST-CSRC (2017).
42 Microsoft (2018b).
43 US NIST-CSRC (n.d.b).

3.2 NATURE AND TAXONOMY OF ICT-DRIVEN THREATS TO SUPPLY CHAINS

The scope and nature of the threat, as well as the taxonomy and major characteristics of ICT supply chain attacks, are better understood with reference to standardized definitions and taxonomy models used by industry and government agencies. The definitions in Table 3.1 are used to define supply chain attacks; however, they are not necessarily specific to ICT supply chains or cyberattack vectors.

Table 3.1 - Definitions of Supply Chain Attacks

DEFINITION	AUTHOR (ENTITY)	SOURCE
Attacks that allow the adversary to use implants or other vulnerabilities inserted prior to installation 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 Committee on National Security Systems (government)	Committee on National Security Systems (CNSS) Glossary, CNSSI 4009-2015
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, distribution) for the purpose of introducing an exploitable vulnerability.	Open Trusted Technology Forum (private sector/technology community)	Open Trusted Technology Provider Standard (O-TTPS), Version 1.1, Mitigating Maliciously Tainted and Counterfeit Products, July 2014
An intentional malicious action (e.g. insertion, substitution, modification) taken to create and ultimately exploit a vulnerability in ICT (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, 2017

Other reports and regulatory guidelines provide definitions with a clearer focus on ICT or cyber supply chain risk taxonomy and attack vectors. For example, according to the US NIST, an ICT supply chain compromise is "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."[44]

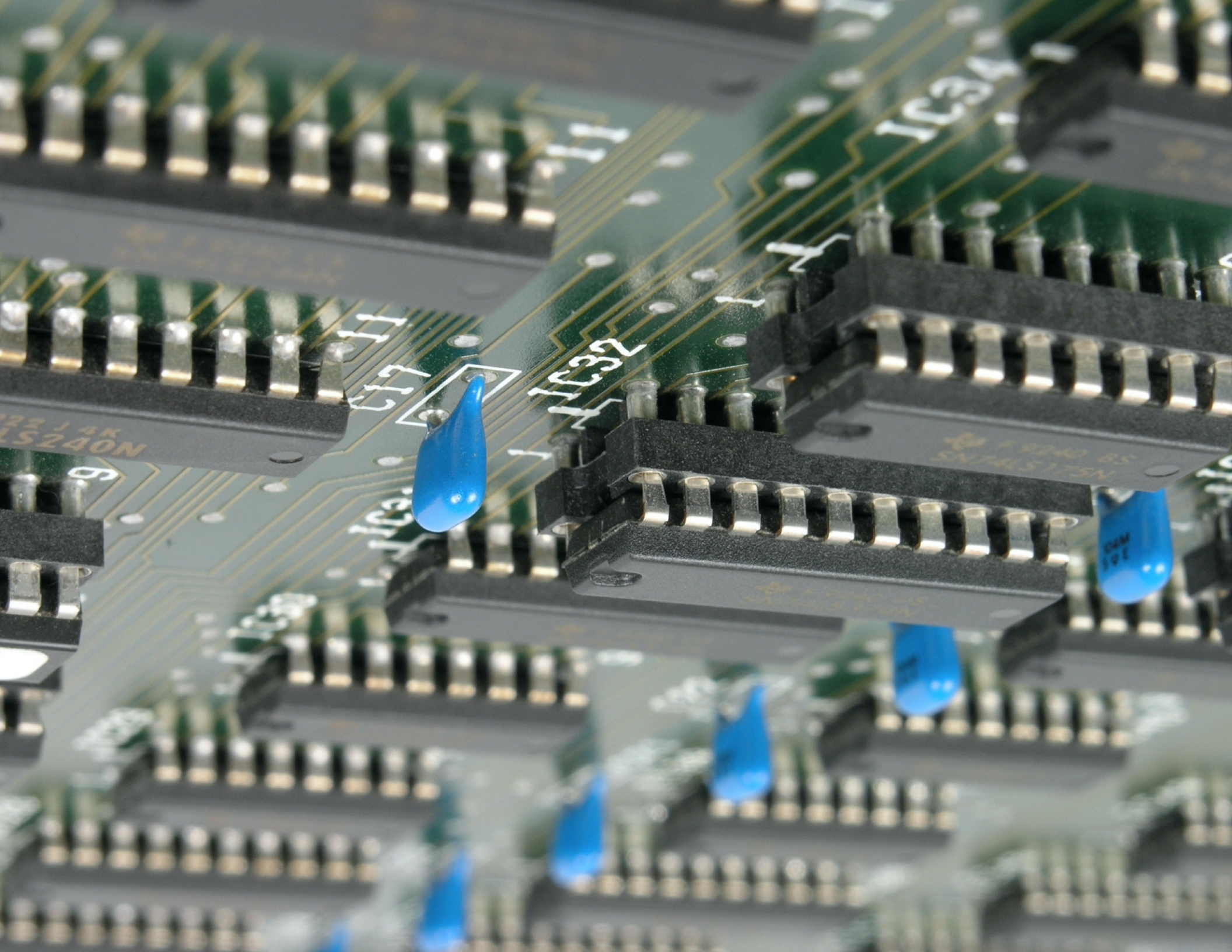
Drawing from the definitions and taxonomies above, we suggest a baseline categorization of ICT-driven threats to supply chains based on the following criteria:[45]

- *Goal of the malicious actor*: ICT supply chain attacks are generally aimed at acquiring unauthorized access to trusted ICT components or systems (hardware, firmware, software or IT-enabled processes) during some stage of their life cycle, before products are shipped or services are delivered to final customers, and modifying those components or systems either to take advantage of existing vulnerabilities or to plant new vulnerabilities and malware.[46] This can be achieved in different ways. An example categorization of methods used by malicious actors is provided by The MITRE Corporation on the basis of 41 case studies of supply chain attacks:[47]
  - *Insertion*: Adding additional information, code or functionality to an ICT module or component that performs a new, malicious function or otherwise subverts the intended system functions. For example, adding malicious code to a software library. Most attacks of this type are applicable to systems under development or during upgrades, updates or the addition of new functionality to the system or its module.
  - *Substitution*: A complete replacement of a module or component (hardware, software, firmware) to be integrated into the system with one that has already been tampered with in order to maliciously change its intended function or operation.
  - *Modification*: Any change to the existing design or other information that defines the system under development. In most cases, the change will cause a degradation or weakness in later developments or production.

44 Boyens et al. (2015).
45 Paulsen (2013).
46 See also: Kavanagh (2019).
47 Heinbockel et al. (2017).

- *Segment of the organization's supply chain and stage of the life cycle of its ICT products or services targeted by the malicious actor*: Attackers can take advantage of vulnerabilities almost within each segment of the supply chain, which raises the need for organizations and their networks of vendors to provide end-to-end security assurances.
- *Type of ICT asset targeted by the supply chain attack*:
  - Software.
  - Hardware or firmware.
  - ICT-enabled processes or services.
- *Role of third-party vendors in the security incident affecting the organization's ICT supply chain*: The nature of the actor behind an ICT supply chain attack can be differentiated according to this specific ad hoc criterion. Two scenarios are possible here:
  - Most recent significant incidents (e.g. Floxif, Kingslayer, NotPetya, ShadowHammer; see Annex VI in the Technical Compendium for more information) are examples of supply chains being targeted and breached by external attackers. Once the malicious actor had successfully exploited vulnerabilities in the vendor's supply chain, the inability of the vendor to promptly identify and mitigate the incident led to the proliferation of the attack to the vendor's client network, to which tampered or modified ICT products were delivered.
  - However, vendors might play a different role in cases where they are aware of vulnerabilities, malware or hidden functions in their software or hardware products or services, and purposefully ship such products or deliver such services to third-party organizations. In such cases, vendors become malicious actors themselves, breaching the security of their clients' ICT supply chains with tainted products or services. This malicious vendor scenario might have relevance in terms of the GGE 2015 norm, which particularly addresses the need to prevent the use of harmful hidden functions in ICT products.

Supply chain attacks, which once used to be a relatively exotic cyberattack vector, have turned into a commonality of the cybersecurity industry – and the cyber-criminal world. The growing number and scale of incidents caused by such attacks might be an indicator that despite the technology industry's best efforts, there is a gap between the speed and capabilities of malicious actors who are increasingly targeting ICT supply chains and the options and strategies available to those defending themselves, their partners and their users against such malicious activities.


IC34
IC32
C11

CURRENT RESPONSES TO ICT-DRIVEN CHALLENGES TO SUPPLY CHAIN SECURITY AND INTEGRITY

4.1 ECOSYSTEM OF STAKEHOLDERS' RESPONSES

In a situation where international norms are just being shaped or are present in a nascent form, stakeholders such as industry actors, the technology community and governments either rely on available tools and strategies to mitigate threats to their supply chain or develop such tools themselves.

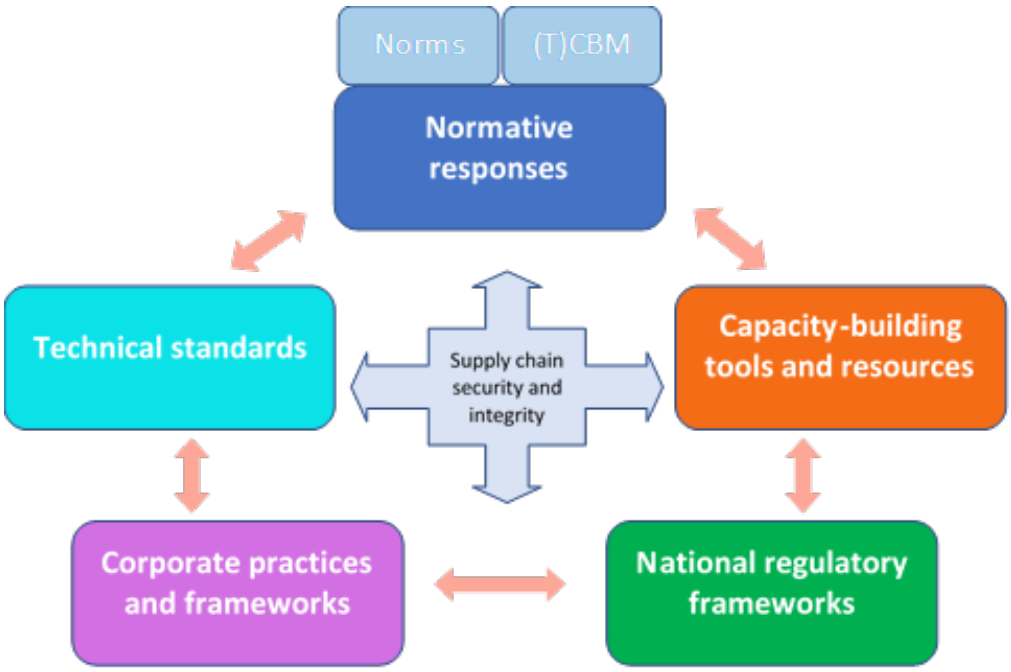
The ecosystem of responses available to States, industries and other stakeholders is multi-tier and complex, with many such responses and frameworks aiming at global impact and adherence. Within this ecosystem, it is possible to identify five categories of responses:

- Norms
- Technical standardization frameworks
- National legislative and regulatory frameworks
- Corporate supply chain security management and supply chain security assurance policies
- (Self-)assessment tools, guidelines, compendiums of best practices and other capacity-building tools and resources

In addition to these elements, there are other tools and incentives for different stakeholders – such as the economic incentive that could be used by regulators to make actors in the private sector change their behaviour and shift to more mature and comprehensive cyber-SCRM policies (e.g. the US Department of Defense's Cybersecurity Maturity Model Certification for defence contractors).

The nature of this ecosystem is not strictly hierarchical; it could, rather, be represented as a set of interconnected, mutually impacting and supporting elements (see Figure 4.1).

Figure 4.1 - Ecosystem of elements for supply chain risk mitigation



Note: (T)CBM = (trust and) confidence-building measure.

- National regulatory frameworks both draw from widely adopted international standards and contribute to shaping them. One example relevant to supply chain security and integrity is the Common Criteria standard, adopted by the International Organization for Standardization (ISO) and historically born from three national and regional information security standards: Canadian, European and US.[48]
- Industry-led standardization frameworks can also evolve into international standards, such as the Open Trusted Technology Provider Standard (O-TTPS), also adopted by ISO and the International Electrotechnical Commission (IEC) in 2015.[49]
- International standardization bodies, such as ISO and IEC, do not develop standards by themselves. The standard development processes, including supply chain security and integrity, are led and shaped by experts in the technical committees and working groups of standardization bodies. Most of these experts come from industry and the technology community, pursuing and promoting the approaches, visions and standardization initiatives of their organizations.

48 See for details: Annex III of the Technical Compendium to this report.
49 See for details: Annex III of the Technical Compendium to this report.

- As demonstrated by multi-stakeholder norm-developing initiatives led by the Global Commission on the Stability of Cyberspace, Microsoft, Siemens, and private actors, industry and technology community actors can also enter the territory of norms development and lead initiatives aimed at multiple stakeholders, including States.

In the supply chain security and integrity field, norms have started to emerge much later and, so far, have gained less maturity than other elements. This is a natural process for many ICT-related sectors, and for information security in general.[50] A detailed description of the nature and scope of normative responses to ICT-driven challenges to supply chains are further explored in Chapter 5 of this report. The following sections in this chapter provide an overview of all the other elements: technical standardization, national regulatory policies, corporate practices, and capacity-building. Such elements can be considered as important pillars of the operationalization of cyber norms related to supply chain security.

4.2 TECHNICAL STANDARDIZATION

In the most simplistic terms, technical standards can be described as a common language used to communicate expected levels of performance for products and services; in the context of this report, these products and services would be within the supply chain flow.[51] The standards, and the institutional frameworks behind them, are among core pillars for complex technology-based ecosystems, the global supply chain being no exception. The supply chain standardization ecosystem is complex and heterogeneous. It encompasses international, regional and national frameworks and related government-adopted standards, as well as industry-led frameworks and initiatives, some of which are also adopted and used internationally and even globally.[52]

Technical standards, however, do not exist in a vacuum and do not induce changes in the supply chain-related practices and processes of organizations by themselves. Standardization is supported and promoted through compliance and certification – practices that exist and evolve in the nexus between standardization, national regulatory policies and internal corporate regulations and practices.

The key specific feature of supply chain security and integrity as a technical standardization sector is that it was initially developed in an ad hoc manner, at the intersection of larger standardization areas.[53] Those include:

50 UNGA (1999); UNODA (2019b).
51 Bartol (2011).
52 Davidson (2014).
53 See: Bartol (2011); Co-Chairs of ANSI's JTC/CS1-ICT SCRM AdHoc Working Group (2017).

- Information security standardization in its broad understanding, covering guiding principles for ensuring the information security and cybersecurity of organizations, systems and processes
- Risk assessment and risk management standards (with a focus on information security and cybersecurity risk management and risk governance)
- Product and services life cycle standards
- Systems engineering standards, covering different aspects of IT systems (e.g. software, computer applications, IT hardware and equipment)

Over the years, however, as ICT-related challenges to global supply chain security and integrity mounted, a push for specific standards was made, resulting in several standardization frameworks with a specific focus on supply chain security management in the ICT context. Major contributions to this process were made by industry experts and governments through the framework of ISO, particularly its Technical Committee 1 (Information Technology) and its Subcommittee 27 (IT Security Techniques), as well as some other major standardization initiatives, such as the Open Trusted Technology Provider Standard (O-TTPS) and ISO/IEC 20243 (see details in Annex III of the Technical Compendium).[54]

A snapshot of the security and integrity of the TSC standardization landscape is provided in Annex IV of the Technical Compendium.

In summary, several challenges to standardization as a major element of the supply chain security and integrity ecosystem can be identified:

- *Most standards, even those with a specific focus on supply chain security in the ICT context, are not ready-made tools that could be instantly adopted and used by organizations*. The guiding principles and requirements, especially in ISO standards, are mostly of a baseline level and are generic in nature. This is inevitable, since no international standard can encompass and reflect the specifics of business processes across the enormous number of sectors, industries, markets and jurisdictions involved in TSC. Therefore, the practical use of a standard for a supplier or buyer depends on its capacity to be adapted to the supplier or buyer's own processes and business niche – and on the actor's motivation.

54 ISO (2019).

- *For standardization, the key tool that helps achieve practical impact on organizations' practices is certification*. The key challenge here is that for many standardization frameworks, such certification is still not imposed as a mandatory requirement by acquirers, both from the commercial and government sectors. In some sectors with heavy governmental regulation, such as defence and aerospace, the situation can be different, but certification for suppliers in such sectors is mostly based on national sector-specific standards and regulatory requirements, not necessarily conformant with global standards.
- *The speed of processes is another challenge to the efficiency of international standardization*. The full cycle of elaboration and adoption of an ISO standard takes 2–5 years.[55] That may not be sufficiently agile, taking into account the dynamics and changing nature of ICT-driven threats to supply chain security and integrity. This could be to a certain extent balanced by the efforts of other standard-developing frameworks, such as 3GPP,[56] NESAS,[57] the German BSI and the European Union standardization bodies (CEN, CENELEC, ETSI).[58] However, these frameworks and their impact on the supply chain ICT standardization landscape could be regarded as complementary to ones developed by the global international standardization bodies, rather than as substituting them.

4.3 NATIONAL REGULATORY POLICIES AND FRAMEWORKS

Governmental regulatory ecosystems encompass legislation and law enforcement provisions; technical regulatory acts and activities aimed at the adaptation and localization of international standards; requirements for actors involved in TSC operation, integrity and security; and compliance frameworks.

In addition to being regulators, governments play a significant role in the multi-stakeholder supply chain ecosystem as a 'big buyer': an actor who controls a large share of the supply chain market ecosystem from the acquirer's side. This role is especially visible in the defence sector and some other industries with an increased level of State-owned assets and extensive governmental acquisition and procurement. Government agencies are sometimes able to use this role as market leverage to incentivize their networks of commercial technology suppliers to adopt best practices for SCRM, security assurance and cybersecurity to enable them to successfully compete for governmental acquisition contracts. As some studies and technical community experts suggest, large

55 Bartol (2011).
56 See: 3GPP (2019).
57 GSMA (2019).
58 EC (2019b); EC (2019c).

public entities that are among the largest acquirers in their national market could perform the role of 'the north star' for vendors in that market.[59]

However, this role should be complemented by a broader collaboration with the private sector, for example for the development of common procurement requirements for ICTs. In addition, the power of governments, both as regulators and major buyers in the technology market, allows them to act indirectly (e.g. by putting pressure on supplier groups) to develop and advance their own industry-recommended practices and conduct self-attestations (including tests of their own products and remediation of vulnerabilities).

As illustrative examples of mature cyber-SCRM regulatory frameworks and policies, overviews of domestic regulatory policies and Governments' efforts to address ICT-driven challenges to supply chains in Japan, the United Kingdom and the United States are provided in Annex V of the Technical Compendium. Some selected highlights are presented below.

4.3.1 UNITED STATES OF AMERICA

- The United States is one of the very few States to address risks to global supply chains at the level of national strategies, with increasing focus on ICT-driven risks.[60]
- The US NIST has developed its *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework). Its Version 1.1.,[61] released in 2018, has significantly expanded its focus on supply chain cybersecurity risk management.[62]
- Today, the framework, used by 30 per cent of US organizations, and by organizations in over 20 other States, serves as a de facto global risk-based tool, allowing its users to identify and map cybersecurity standards, best practices and other tools for their type, specific sector and business process, covering the cyber SCRM (C-SCRM) niche.[63]

59 Nissen et al. (2018).
60 US White House (2018).
61 US NIST (2018b).
62 For a detailed overview of the framework's methodology, see Annex V to this report, bullet point 1.
63 US NIST (2018a).

- Dedicated C-SCRM frameworks have also been developed. The US NIST C-SCRM Programme[64] was launched in 2008 in response to Comprehensive National Cybersecurity Initiative No. 11, '*Develop a Multi-Pronged Approach for Global Supply Chain Risk Management*'.[65] More recently, special focus has been placed on establishing requirements to mitigate supply chain risk to the US Department of Defense's critical systems and functions.[66]

4.3.2 UNITED KINGDOM

- The Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) provide guidance for ICT risks involving contractor–supplier relationships (e.g. cloud security principles, insider threat study).[67] The CPNI and NCSC recommendations aim to help organizations secure their own systems themselves, instead of ensuring direct responsibility and comprehensive control of the Government over SCRM in the private and non-governmental sectors.
- Most tools and resources addressing ICT supply chain security in the United Kingdom are not purely governmental or regulatory instruments but the products of public–private partnerships; for example:
  - CyberEssentials,[68] a set of basic technical controls to help organizations protect themselves against online security threats, developed by the UK Government in collaboration with the private sector (SME and cybersecurity associations).
  - The Trustworthy Software Initiative,[69] supported by the UK Government's National Cyber Security Programme, aims to help promote trustworthy software among the supply, demand and education communities in a risk-based, whole life cycle process.

64 US NIST (2018c).
65 US White House (2019a).
66 Under Secretary of Defense for Acquisition and Sustainment (2019); US DoD (2018).
67 CPNI (2019).
68 NCSC (2019).
69 Trustworthy Software Foundation (2019).

4.3.3 JAPAN

- The approach to mitigation of risks related to the technological transformation of the global supply chain and the whole IT sector is shaped on a strategic and conceptual level in the draft Cyber/Physical Security Framework, released in 2019 by the Ministry of Economy, Trade and Industry.[70] The framework serves as a major cybersecurity pillar behind the programme 'Connected Industries', launched by the Japanese Government to create value by building connections among disparate industrial data.[71]

The analysis of national approaches could serve as a useful springboard for other governments willing to strengthen their regulatory frameworks. It would also be particularly insightful to conduct an overview of States that do not have well-elaborated strategic, policy and regulatory frameworks in this field. The overview of such frameworks across all United Nations Member States goes beyond the scope of this report, and such comprehensive information was not identified in existing literature.

4.4 CORPORATE PRACTICES AND FRAMEWORKS

Corporate sector activities include extensive toolkits of requirements to vendors and elaborated procedures, guidelines and best practices aimed at the minimization and mitigation of ICT-related risks in corporate supply chains. Technical supply chain security assurance frameworks developed by commercial enterprises and other actors in the private sector focus on different segments of the supply chain ecosystem:

- *Upstream supply chain security assurance*: This assurance framework encompasses tier 1 vendors who supply products, components or services to an organization, and to further tiers of suppliers.
- *Downstream supply chain security assurance*: In this model, an organization aims to demonstrate assurance to its customers, or acquirers, and develop a framework that would enable it to demonstrate that its own supply chain was not compromised or breached.
- *Comprehensive or end-to-end supply chain security and integrity assurance*: These frameworks cover both upstream and downstream segments of corporate supply chains. However, developing and maintaining such frameworks is an increasingly difficult task that requires considerable resources and skills from organizations. For large corporations, the complexity of end-to-end supply chain assurance increases proportionally to the number of its upstream suppliers and downstream acquirers.

70 METI (2019a).
71 METI (2019b).

Examples of such practices deployed by industry can be best reviewed and summarized by looking at large technology sector corporations with vast transnational supply chains and a large number of both suppliers and clients (upstream and downstream supply chains). As illustrative examples, in this section we provide an overview of initiatives by three large technology corporations based in East Asia (Huawei), North America (Microsoft) and North Eurasia (Kaspersky). More information on these three industry players is provided in Annex VI of the Technical Compendium.

This overview does not provide a comprehensive understanding of ICT-focused supply chain assurance and risk management practices throughout the global technology industry. However, because of the scale of these enterprises and their leading positions in their market niches, it is intended to illustrate at least certain key trends and approaches towards TSC risk management and the strengthening of TSC security, integrity and transparency.

A good compendium of other private sector practices was prepared by the US NIST through its project 'Industry Best Practices for Cyber SCRM',[72] which provides a detailed overview of supply chain risk management approaches by Cisco, DuPont, FireEye, Fujitsu, Intel, Juniper, Northrop Grumman[73] and other industry players.

4.4.1 HUAWEI

Huawei has developed a comprehensive company-wide approach encompassing security assurance of its products and business processes,[74] with its key components and pillars being:

- *Company-wide coordination and division of responsibilities in security assurance*, with a central body – Huawei's Global Cyber Security Committee – having responsibility over Huawei's security assurance programme, including its ratification, strategic planning, policies, roadmap, investment and implementation.[75]
- *Integration of security assurance throughout the company's business processes*, including research and development, the supply chain, sales and marketing, delivery, and technical services.

72 US NIST-CSRC (2019a).
73 US NIST-CSRC (2019h); see also: US NIST-CSRC (2019a); US NIST-CSRC (2019b); US NIST-CSRC (2019c); US NIST-CSRC (2019d); US NIST-CSRC (2019e); US NIST-CSRC (2019f); US NIST-CSRC (2019g).
74 Suffolk (2013).
75 Suffolk (2013, 11).

- *Major focus on national and international standardization and certification frameworks*, including compliance with standards for internal auditing, and receiving external certification and auditing from security authorities and independent third-party agencies (including use of and compliance with such international standards as ISO-9001, ISO-14001, ISO-27001 and ISO-1540).[76]
- *Additional mechanisms to address supply chain security risks*, including the Internal Supplier Cyber Security System Qualification standard, based on ISO-28000;[77] the corporate Supply Chain Cyber Security Baseline framework, covering requirements on physical security, software delivery security, organizational processes, and personnel security awareness; [78] and 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 the corporate supply chain.[79]

In parallel with developing upstream quality control and SCRM mechanisms, the company's major efforts since the early 2000s have been also aimed at creating frameworks to provide downstream security assurances and at ensuring trust in its products among users, partners and governmental authorities in the company's markets.[80]

4.4.2 MICROSOFT[81]

Microsoft's Supplier Assessment Program[82] uses a combination of supplier risk profiling and focused control-based assessments, including a system of risk indicators, scoring, risk profiles and recommended courses of action. These include:

- *Policies, standards and control procedures*: These procedures apply to software, goods and services from third-party suppliers.
- *Supplier risk profiling model*: Microsoft has developed a system of dashboards containing at-a-glance information about each supplier and the health of the products or services they offer to the company.

76 See: Purdy (2016); see also: Annex III, bullet point 10, in Technical Compendium to this report for details.
77 ISO (2007a); ISO (2007b).
78 ISO (2007b, 22–23).
79 ISO (2007b).
80 See: Huawei Cyber Security Evaluation Centre Oversight Board (2019, part I).
81 In the context of this report, Microsoft's internal corporate practices in supply chain security management should be analysed separately from the corporation's efforts to launch – or to contribute to – norm-developing initiatives and cross-sector solutions for cybersecurity. Although some of these initiatives (e.g. Cybersecurity Tech Accord, Digital Geneva Convention) directly or indirectly address supply chain security and integrity, they are different from the internal practices and management approaches deployed across the corporation's supply chain.
82 Microsoft (2017).

- *Integrating assurance into the procurement life cycle*: The Program[83] integrates security escalations to ensure that Microsoft chooses secure third-party software, goods and services from trusted suppliers.

4.4.3 KASPERSKY

The company's Global Transparency Initiative[84] was launched in 2017 as a response to accusations made against the company of cyber espionage and deploying hidden data exfiltration functions into its cloud-based cybersecurity products and services sold to Western markets, notably the United States[85] and the United Kingdom.[86]

- Although the Global Transparency Initiative does not exclusively focus on SCRM or explicitly mention it, it 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.
- The company's initiative is aimed at engaging the broader information security community and other stakeholders in validating and verifying the trustworthiness of its products, internal processes and business operations. Key measures implemented as part of the initiative include:[87]
  - Allowing independent review of Kaspersky's source code, software updates and threat detection rules by governments and accredited experts on request.
  - Allowing independent review of Kaspersky's secure development life cycle processes and its software and supply chain risk mitigation strategies.
  - Deploying Kaspersky corporate Transparency Centers globally to address any security concerns together with customers, trusted partners and government stakeholders.[88]

83 Microsoft (2017); Microsoft (2019).
84 Kaspersky (2019).
85 115th US Congress (2017); Office of the Press Secretary (2017); DoD, GSA & NASA (2019).
86 Martin (2018).
87 Kaspersky (2019).
88 The first Transparency Center 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. The second Transparency Center was launched in Madrid in June 2019. By early 2020, the company plans to open its third Transparency Center in Kuala Lumpur, expanding its initiative to Asia Pacific.

Some **generalized findings** from this overview of corporate best practices include:

- Most top-level corporate players have developed comprehensive and detailed internal frameworks to address potential risks coming from upstream suppliers. These frameworks combine general risk management methods, vendor assessment and certification tools, upstream supply chain traceability systems and other elements. While this level of maturity among top industry actors is certainly a positive trend, it might also pose some challenges. For example, if requirements are not harmonized across industry actors, suppliers will face an increased administrative cost resulting from different compliance obligations. For SMEs, this compliance burden might be beyond their organizational capacity. In more general terms, this observation identifies **the need for greater harmonization** of ICT-focused SCRM frameworks across the industry, especially in the upstream segment, which encompasses the dispersed community of technology suppliers with a major share of SMEs.
- Downstream SCRM and assurance has become a major area of concern, with more and more governments considering or taking legal action to mitigate potential risks stemming from ICT products shipped to their national markets by global technology suppliers. In this area, even large corporations are in the process of developing dedicated assurance frameworks to address and resolve governmental concerns across national markets (e.g. Huawei, Kaspersky).
- Governments and global technology vendors might benefit from a sort of 'framework of frameworks' to standardize the scope, methodology and underpinning principles of requirements for global technology suppliers to enable them to demonstrate security assurance across national jurisdictions through a uniform approach.

4.5 CAPACITY-BUILDING TOOLS, RESOURCES, GUIDES AND BEST PRACTICES

Capacity-building for the purpose of this report is understood as the development and strengthening of human and institutional resources.[89] Capacity-building tools and resources are often referred to in the discussions of the GGE and, recently, the OEWG.

Developing capacities does not require a normative basis per se and could be implemented by multiple actors without any consensus on underlying norms. Examples include capacity-building activities conducted by private sector actors among networks

89 OECD (2018).

of their suppliers as part of their efforts to ensure responsible supply chain management and governance.

Multiple useful resources, capacity-building tools, compendiums of best practices and guidelines exist to help organizations better understand and manage ICT-driven supply chain risks. Some relevant examples include:

- *(Self)-assessment and auditing tools and services for cyber-SCRM*: Such tools help organizations navigate legal and regulatory requirements to SCRM and supply chain security assurance, seek conformance with major national and international standards, better understand the effectiveness of their cyber-SCRM practices, and identity improvement opportunities. A series of such tools with different specializations was developed by industry, the technology community and regulators to assist organizations in understanding and implementing the US NIST Cybersecurity Framework (see Annex VII of the Technical Compendium for descriptions of a select number of such tools).
- *Digital platform solutions for secure collaboration and information-sharing among vendors*: Such platforms enable organizations to assess, measure and mitigate risk in real time across multi-tier partner and supplier networks, with a focus on cybersecurity risks (e.g. see the Exostar Risk Management Solution, as described in Annex VII of the Technical Compendium).
- *Volunteer SCRM and security assurance frameworks*: Volunteer frameworks and methods developed by industry and the technology community to help organizations manage their supply chain risks (e.g. see the Software Supply Chain Integrity Framework[90] developed by the Software Assurance Forum for Excellence in Code (SAFECode), a global, industry-led non-profit organization working to increase trust in ICT products and services with key focus areas including software development, integrity controls and supply chain security).
- *Research publications, guides and compendiums of best practices in SCRM and supply chain assurance*: A wide spectrum of publications exist that do not have legislative or regulatory status but are intended to provide advice and recommendations to different actors on how to advance their practices and better mitigate ICT-driven risks to supply chains. Some notable examples include:
  - *North American Transmission Forum Cyber Security SCRM Guidance*:[91] This publication aims to summarize best practices for establishing and implementing a cyber-SCRM plan.

90 SAFECode (2009).
91 NATF (2018).

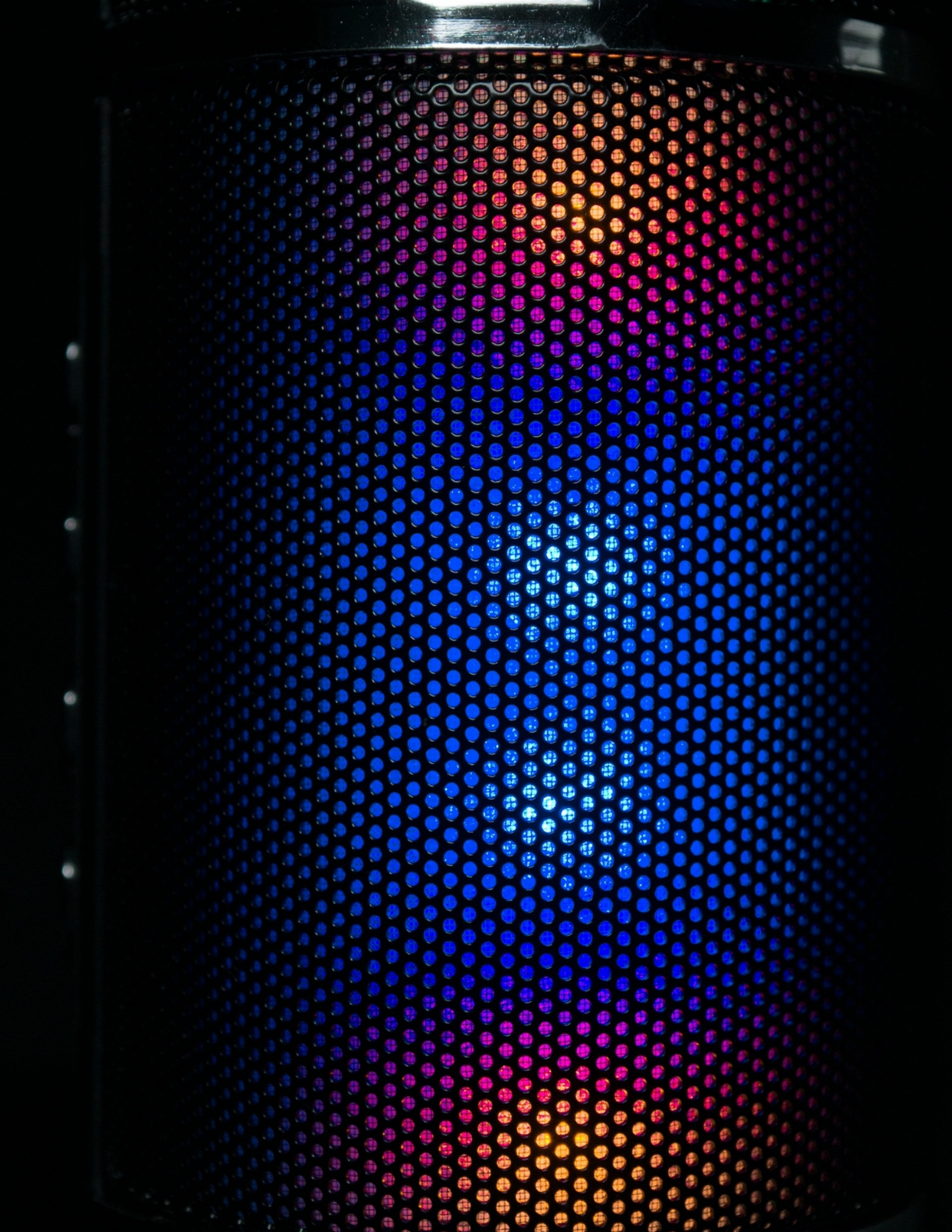
- *Deliver Uncompromised*:[92] This report by the MITRE Corporation provides an in-depth overview and assessment of challenges that the US Department of Defense and the intelligence community have been facing with regard to ensuring the security and integrity of their cyber supply chains.
- *Cyber Product International Certification Commission Initiative*:[93] Developed by the Electric Infrastructure Security Council, this initiative aims to provide electric infrastructure operators in the United States with a comprehensive process, driven by industry and other stakeholders, to certify that crucial hardware and software products are minimally scrubbed of malware and other means of adversary exploitation.
- *Purchasing Secure ICT Products and Services: A Buyers Guide Version 1.0*:[94] This guide, produced by the EastWest Institute, with support from a number of technology sector companies, is intended to provide a compendium of best practices and guidelines for organizations, as well as for individual users, to help them better understand and address the cybersecurity and privacy risks related to ICT products and services and their supply chains.

Such tools and publications, with all their diversity, are an important component in the effective adoption and advancement of supply chain cyber risk management practices by commercial entities, as well as by governmental agencies and regulators. However, three gaps can be identified with regard to current trends in the development and use of such tools and resources:

- The majority of such tools and resources address particular national markets, regulatory frameworks and national standards, with the United States and its NIST Cybersecurity Framework being absolute leaders. However positive for the world's largest technology markets, this leaves most other States, especially those with lower capacities, cut off from the best practices, knowledge and tools that their own industries and regulators might need to mitigate ICT-driven risks to supply chains.
- A major share of such tools and resources is focused on specific sectors with heavy governmental regulation and complex security processes and requirements (e.g. defence, federal acquisition). While this is not entirely surprising, it may result in an increasingly patchy and incoherent development of cross-sector and, possibly, internationally adopted cyber-SCRM frameworks.

92 Nissen et al. (2018).
93 Stockton (2018).
94 EastWest Institute (2016).

- The actual efficiency, effectiveness, reliability and overall value of such tools need to be verified and asserted through independent assessments and evaluations to ensure that they do not wrongly become substitutes for more effective, yet resource-intensive processes.



NATURE AND SCOPE OF NORMATIVE RESPONSES TO ICT-DRIVEN CHALLENGES

The last element of the supply chain risk mitigation ecosystem is represented by international responses, which can be divided in three types, as described in the reports of the GGE on cybersecurity and in studies by cyber norm experts.[95]

- *Norms*: As defined by the World Bank (see Section 1.1), norms are the shared expectations or standards of appropriate behaviour accepted by States and intergovernmental organizations (IGOs) that can be applied to States, IGOs and non-State actors of various kinds.[96]
- *Trust and confidence-building measures (TCBMs)*: The notion of (T)CBMs was adapted to the context of international negotiations on ICT security from Organization for Security and Co-operation in Europe (OSCE) practices, where it is used in the context of conflict prevention. As such, CBMs do not have a commonly accepted definition,[97] although they are categorized into military and non-military CBMs.[98] However, neither the global technology industry nor the regulators refer to this notion when discussing practices and mechanisms for addressing ICT-driven challenges to supply chain security and integrity. This issue is further addressed in Chapter 6 (see Gap 7).
- *Capacity-building*: As already discussed in discussed in Section 4.5., capacity-building is a separate pillar of the ecosystem, although complementary to other normative responses.

5.1 OVERVIEW OF NORM-DEVELOPING INITIATIVES ADDRESSING SUPPLY CHAIN SECURITY AND INTEGRITY

The norm-developing initiatives intended to strengthen security and integrity in the supply chain, and mitigate ICT-driven threats to it, emerge from different processes and stakeholders.

Major intergovernmental discussions are taking place under the United Nations auspices, continuing the work of the previous five GGEs on cybersecurity. Supply chain issues in the

95 Osula & Rõigas (2018).
96 Martinsson (2011).
97 OSCE (2012, 9).
98 OSCE (2012, 9).

context of ICT-driven threats were first addressed by the third GGE's report in 2013. Today, they are emerging in the discussions conducted by both the GGE and the OEWG on cybersecurity. For example, in its submission to the first substantive session of the OEWG, which took place in New York on 3–4 September 2019, China stated that supply chain security is crucial for enhancing user confidence and promoting the digital economy and proposed some specific norms related to supply chain security.[99]

Regional organizations and other multinational groupings have also paid attention to supply chain issues in the context of ICT security and international cooperation. Examples include:

- The Shanghai Cooperation Organisation (SCO) called on States to endeavour to ensure the supply chain security of ICT goods and services in its revised International Code of Conduct for Information Security, dated 2015.[100]
- The Group of Seven (G7) supported the set of norms from the GGE 2015 report and stated its commitment to their implementation in its Dinard Declaration on the Cyber Norm Initiative, adopted in 2019.[101] This includes norms concerning supply chains, although not explicitly mentioned in the text. In addition, the G7 also adopted its *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* in October 2018.[102] Although this effort is sector-specific and focused on the concept of third-party risk management, it covers most of the supply chain security management issues within the financial sector.

Finally, an increasing number of norm-developing initiatives addressing supply chain security and integrity in the context of ICT-driven risks come from multi-stakeholder initiatives – the 'norm entrepreneurs'. Such initiatives include:

- Microsoft's initiative, the Digital Geneva Convention to protect cyberspace, calls on States to refrain from inserting or requiring 'backdoors' in commercial off-the-shelf products.[103]
- The Cybersecurity Tech Accord initiative, also launched by Microsoft and other major technology companies, is indicative of the commitment of its participants to protect users and organizations against tampering with technology products and services.[104]

99 UNODA (2019a).
100 UNGA (2015).
101 G7/8 (2019).
102 G7 (2018).
103 Microsoft (2018a).
104 Cybersecurity Tech Accord (2019).

- The cybersecurity Charter of Trust, a global industry-led framework launched by Siemens, aims to ensure responsibility throughout the digital supply chain, promotes security certification and sets minimum binding security requirements for suppliers.[105]
- The Global Commission on the Stability of Cyberspace (GCSC) in its 2018 Singapore Norm Package calls on States and non-State actors to refrain from tampering with products and services in development and production.[106]
- The Paris Call for Trust and Security in Cyberspace, launched in 2018 by the French Government, with support from technology sector companies, includes a commitment to strengthen the security of digital processes, products and services throughout their life cycle and supply chain.[107]

A more detailed overview of these frameworks and their normative initiatives addressing supply chains is provided in Annex VIII of the Technical Compendium.

5.2 COMPARATIVE ANALYSIS OF SUPPLY CHAIN NORM-DEVELOPING EFFORTS

In comparing the scale and scope of the above-mentioned initiatives, some key factors were identified, including:

- Altogether, international norm-developing initiatives that explicitly address the security and integrity of ICT supply chains or mitigation of the risk posed by hidden functions and backdoors in ICT products have been fostered by eight transnational actors.
- Most of them (five out of eight) are multi-stakeholder normative cybersecurity frameworks developed and led either by technology industry actors (Microsoft, Siemens) or by mixed stakeholder groups including both States and technology sector actors (Paris Call). This reflects a major trend towards industry and the technology community proactively contributing to the normative agenda for cybersecurity in different niches and taking the lead in the promotion and implementation of such initiatives.
- Regional organizations appear to be the most underrepresented of the actors addressing ICT supply chain security and integrity issues from a normative perspective. The only regional organization addressing supply chains in the context of information security is the SCO in its revised International Code of Conduct for Information Security.

105 Siemens (2019).
106 GCSC (2018).
107 France Diplomatie (2018).

- Most of the initiatives are 'positive' norms by their modality (i.e. provisions encouraging or binding States to do something); two initiatives are examples of 'negative' norms, calling States or other actors to avoid or to refrain from certain actions. One normative provision that is difficult to categorize as positive or negative is the proposed norm on ensuring ICT supply chain security in the SCO code of conduct.
- The initiatives, proposed or implemented both by States and by multi-stakeholder forums, can be divided into four categories according to the scope of the supply chain-related security risks or the risk mitigation activities they address:
  - *Initiatives aimed at mitigating harmful hidden functions*[108] *or backdoors*:[109] Such norms focus explicitly on only one type of malicious activity affecting the ICT supply chain.
  - *Initiatives aimed at avoiding tampering with ICT products*: This category of norms is broader than the previous one; tampering could include virtually all attack methods applicable to ICT products, components and services in the supply chain.
  - *Initiatives aimed at ensuring the security and integrity of ICT supply chains*: This category could be regarded as covering the whole spectrum of activities related to ICT SCRM, not limited to the prevention and mitigation of particular attack methods or vectors.
  - Initiatives aimed both at mitigating harmful hidden functions or backdoors and ensuring the security and integrity of ICT supply chains: This category, which includes norms from the GGE 2015 report, addresses supply chain security and integrity issues involving ICTs in a relatively comprehensive manner, mentioning ICT supply chain security in general and identifying priority risks to it.
- The only initiative of binding nature is the cybersecurity Charter of Trust, which includes minimum binding security requirements on suppliers and provisions for mandatory independent third-party certification for critical infrastructure and critical IoT solutions.

Graphic representation of this baseline categorization is available in Table 5.1.

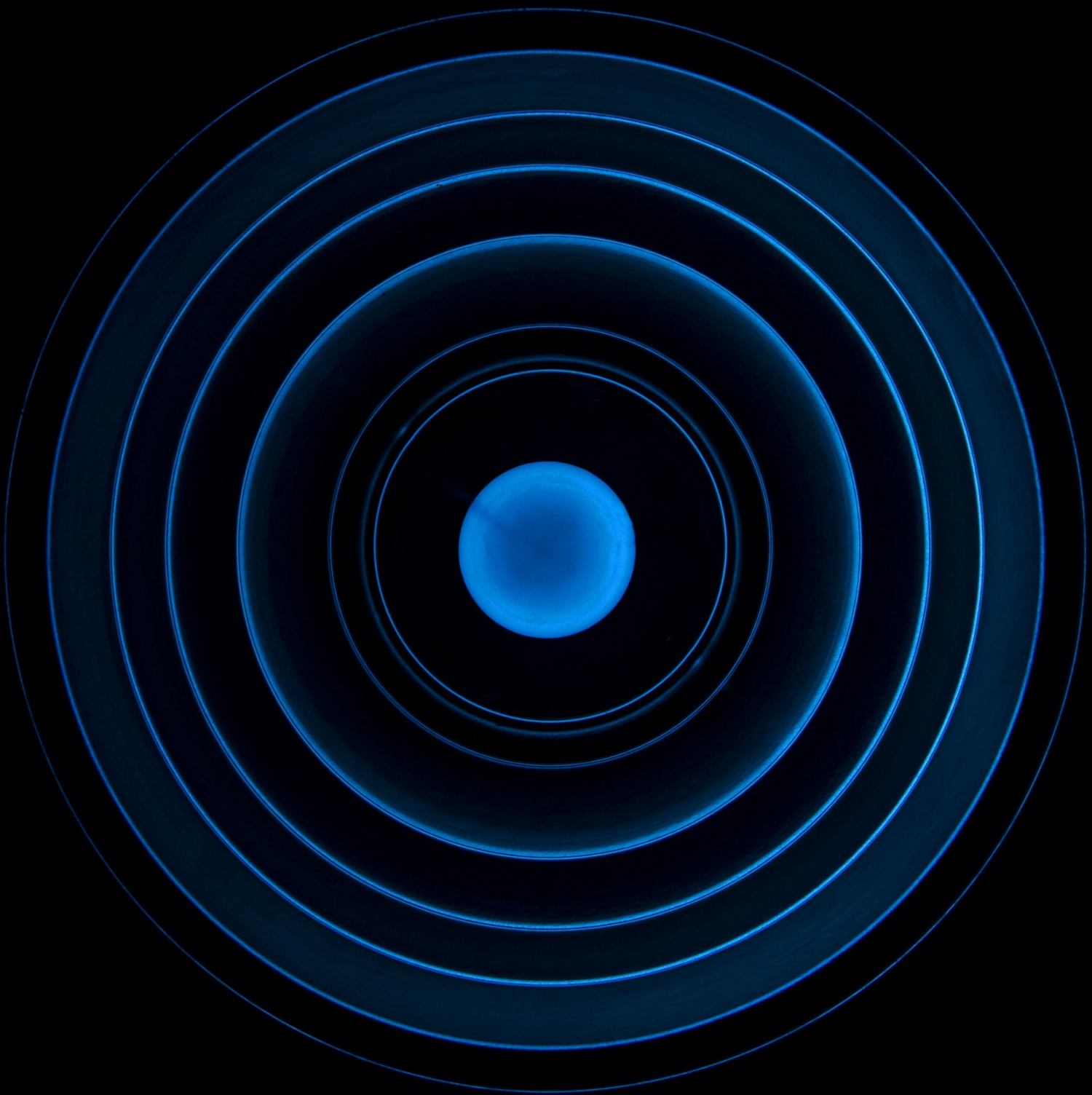
108 For 'harmful hidden functions', no standardized or commonly accepted explicit definition was identified. Contextually, this term is used in the UNGA documents, such as the reports of the cyber GGEs and resolutions on developments in the field of information and telecommunications in the context of international security as synonymous with 'backdoors'.

109 US NIST-CSRC (n.d.a).

Table 5.1 - Categorization of normative initiatives involving ICT-driven risks to supply chain

Initiatives or criteria	Stakeholders		Positive vs negative		Subject scope			
	IGO	Multi	Positive	Negative	Backdoors/ HHF	Tampering	Supply chain S&I	SC S&I + backdoors / HHF
GGE	✓		✓	✓				✓
G7	✓		✓	✓				✓
SCO	✓		✓	✓			✓	
Digital Geneva Convention		✓		✓	✓			
Cybersecurity Tech Accord		✓		✓		✓		
Cybersecurity Charter of Trust		✓	✓				✓	
GCSC		✓		✓		✓		
Paris Call for Trust and Security in Cyberspace		✓	✓			✓		

G7 = Group of Seven | GCSC = Global Commission on the Stability of Cyberspace
GGE = Group of Governmental Experts | HHF = harmful hidden function
IGO = intergovernmental organization | S&I = security and integrity | SC = supply chain
SCO = Shanghai Cooperation Organization



GAPS IN SUPPLY CHAIN NORM-DEVELOPING EFFORTS

This chapter focuses on gaps – or areas for improvement – in normative initiatives or in the courses of action supporting them.

The following gaps in reviewed supply chain norm-developing efforts are identified in this report:

1. Lack of observation incentives and implementation mechanisms for 'negative' norms.
2. 'Patchwork' nature of initiatives focusing on harmful hidden functions.
3. Overlaps and duplication of efforts by multi-stakeholder initiatives.
4. Lack of standardized process frameworks for dealing with global technology vendors in national markets.
5. Lack of coordination and synergy between intergovernmental normative initiatives, global industry and the technology community.
6. Lack of focus on addressing supply chain ICT-driven risks through capacity-building.
7. Lack of focus on using CBM toolkits to address supply chain ICT-driven risks.
8. Overall low level of maturity of national frameworks and initiatives to ensure security and integrity of TSCs.

A concise description of these gaps is provided below; the gaps represent the basis for the recommendations described in chapter 7.

GAP 1: LACK OF OBSERVATION INCENTIVES AND IMPLEMENTATION MECHANISMS FOR 'NEGATIVE' NORMS

- Such norm initiatives are challenged by lack of proper motivation and incentives for compliance among the actors they are targeting. Several reports have indicated that for global norms to transplant and consolidate, a long-term commitment as well as cooperation among a broad range of highly involved stakeholders is crucial.[110] Norms that address harmful hidden functions, backdoors and tampering with ICT products and services in the TSC solely from a 'negative' perspective (banning such activities or requiring actors to avoid or refrain from them) rest on an expectation that States and other actors would voluntarily commit to and observe the norms. This expectation is at odds with the dynamics of the threat landscape in the ICT supply chain. As discussed above, industry and States are witnessing a sharp increase in malicious cyber activities targeting global supply chains.
- Norms that challenge existing practices still can succeed and get a foothold if their agenda setting is accompanied and supported by implementation and monitoring frameworks. For supply chains, comprehensive security assurances and ICT SCRM frameworks could be scaled up to a cross-sectoral and transnational level. However, a norm initiative needs to encompass this 'positive' component and aim to establish such frameworks if they are not currently in place. Norm-developing initiatives that combine negative and positive elements are better suited for operationalization, as positive elements can potentially kick-start the mechanisms necessary for implementation of the negative components.
- The potential for effective observation of negative norms is limited by the well-known challenge of ensuring credible attribution of malicious cyber activities. One of the key tools that could support adherence to negative norms would be 'negative incentives', such as certain forms of legal responsibility, sanctions or other kinds of penalty for violating the norm and conducting harmful activity.

110 Martinsson (2011).

GAP 2: 'PATCHWORK' NATURE OF INITIATIVES FOCUSSING ON HARMFUL HIDDEN FUNCTIONS

- The insertion of hidden functions, software and hardware backdoors presents a major challenge. However, experiences across industry, the technical community and the public sector demonstrate that ICT-driven risks to TSCs should be addressed through comprehensive and integrated C-SCRM, end-to-end security assurance frameworks, and compliance programmes. This includes identifying and mapping the entire spectrum of risks and developing strategies to address them within a holistic set of SCRM policies, practices and tools.
- Norms with a scope limited to backdoors do not fit into this kind of holistic approach, as they set the hidden function risks apart from the rest of the ICT-driven risks to supply chains and thus break the paradigm of an integrated and comprehensive risk management approach.

GAP 3: OVERLAPS AND DUPLICATION OF EFFORTS BY MULTI-STAKEHOLDER INITIATIVES

- As reflected in the mapping of industry-led and multi-stakeholder normative initiatives (see Table 5.1), many of those initiatives (Tech Accord, GCSC Norm Package, Paris Call) address ICT supply chain issues from a similar perspective and identify overlapping approaches and norms. This is accompanied by a significant share of major technology corporations, which are shaping the backbone of global ICT supply chains, being engaged in several such initiatives in parallel.
- While diversity of frameworks and initiatives, and even certain competition among them, boosts the global cybersecurity norm-developing agenda, it could also result in dispersion of efforts. In particular, this trend generates the risk of multiple parallel SCRM and security assurance frameworks competing for the status of de facto global standardized practice.[111]

111 Similar phenomena have been observed in some sectors of technical standardization of emerging digital technologies (e.g. standards for wireless networking protocols for IoT infrastructures and services). Competition between major technology consortia within the venues of international standardization bodies has resulted in a complex and highly heterogeneous ecosystem of IoT standardization stacks, lacking interoperability and end-to-end security approaches.

GAP 4: LACK OF STANDARDIZED PROCESS FRAMEWORKS FOR DEALING WITH GLOBAL TECHNOLOGY VENDORS IN NATIONAL MARKETS

- As identified in Chapter 4 of this report, an emerging trend across a small number of governments is the creation of special process frameworks and organizational interfaces (cybersecurity evaluation centres, transparency centres) as 'entry gates' to national markets for global technology vendors. While the establishment of such frameworks could be initiated by vendors in response to regulators' requirements and security concerns, governments are the driving force behind it.
- In terms of potential norm-supporting solutions, the challenge is avoiding the need to develop such frameworks in an ad hoc, customized manner for each major vendor and each jurisdiction where it conducts business. Without a standard (or at least harmonized) approach, the process of establishing such frameworks across national markets might be excessively complex and costly, both for governments and vendors, as well as too long and slow to keep up with the pace of proliferation of ICT-driven threats to global supply chains.
- Such frameworks are not explicitly mentioned in normative initiatives and could not be linked directly to any of them. However, this practice is gradually becoming widespread and mainstream and is driving the logic of supply chain security assurance further into the domain of public–private cooperation – as a type of multi-stakeholder approach. Unlike common top-down logic, where norms serve as a conceptual basis for their implementation frameworks and practical mechanisms, the practice of establishing this new type of process framework might be promoted to a normative status through a bottom-up approach – as a best common solution to handling foreign supplier-related ICT risks for national regulators.

GAP 5: LACK OF COORDINATION AND SYNERGY BETWEEN INTERGOVERNMENTAL NORMATIVE INITIATIVES, GLOBAL INDUSTRY AND THE TECHNOLOGY COMMUNITY

- Intergovernmental initiatives addressing TSC security and integrity through norms emerged much later than industry practices and community efforts (including standardization and certification frameworks). Thus, fundamental concepts such as end-to-end SCRM and security assurance along TSCs, as well as advancement of relevant international standards, are not referred to in the GGE reports or the SCO proposed Code of Conduct of 2015. In contrast, the scope and modality of norms proposed by multi-stakeholder frameworks with States' involvement (e.g. the Paris Call) appear to be shaped by, and take account of, industry and the technology community's perspectives and approaches.
- This gap is also a reflection of the processes used to develop intergovernmental norms. For example, the GGE is, by design, characterized by selected participation and not meant to engage a wider range of stakeholders during its formal meetings. This format has been serving its purpose for years, providing the necessary conditions to achieve difficult consensus on norms for cyberspace in 2013 and 2015. While this lack of inclusiveness should be at least partially addressed through the OEWG, its first substantive session in September 2019[112] did not result in a strong participation of industry or technology community actors.
- The last factor contributing to this gap is the different process modalities of intergovernmental initiatives and activities conducted by the technology community and by industry. While the GGE and the OEWG have time-bound mandates to negotiate (and ideally reach consensus on) specific issues in a limited number of sessions, initiatives in the technology community and in industry are based on a more continuous process requiring permanent engagement, management and governance (e.g. Cybersecurity Tech Accord, cybersecurity Charter of Trust).

112 UN Web TV (2019).

GAP 6: LACK OF FOCUS ON ADDRESSING SUPPLY CHAIN ICT-DRIVEN RISKS THROUGH CAPACITY-BUILDING

- Considering that the ecosystem of technology suppliers is globally dispersed, and many suppliers are based in jurisdictions lacking mature regulatory policies and standardization frameworks, international capacity-building efforts could considerably improve the overall risk environment in global supply chains. However, no norm-developing framework identifies ICT SCRM as a separate, prioritized item on its capacity-building agenda.

GAP 7: LACK OF FOCUS ON USING CBM TOOLKITS TO ADDRESS SUPPLY CHAIN ICT-DRIVEN RISKS

- Like capacity-building, the role that (T)CBMs could play in addressing ICT-driven risks to TSCs has been underexplored. A few expert references to this instrument suggest that (T)CBMs would be hard to apply and verify in the context of the implementation of the GGE norm on supply chain.[113] To a certain extent, this is because the concept of CBMs was shaped for the prevention and mitigation of armed conflicts and still operates with this logic and language, which is quite distant from the language and logic of the vendors, buyers and regulators involved in supply chain relationships.
- Relative success in the adoption of CBMs at the regional level (OSCE in 2012 and 2016) and the bilateral level (US–Russian agreements of 2013) to mitigate transnational ICT-driven risks gives reason to further explore the adaptation of the CBM toolkit to managing cybersecurity challenges for TSCs.
- In terms of key objectives, (T)CBMs have much in common with security assurance frameworks - both methods aim to generate trust between parties interacting in an untrusted environment. Transparency is another common cornerstone for the two approaches: in the CBM context, it is needed to increase understanding between parties and reduce the risk of escalation. In the vendor networks and in the TSC itself, transparency is one of the key aims of SCRM and security assurance.
- Voluntary sharing of information on threats, risks and vulnerability vectors is also part of both (T)CBM and comprehensive SCRM and security assurance methods.
- Voluntary sharing of information on adopted strategies, regulatory measures, best practices, and so on, could be used in the supply chain ICT risk management context both by corporate actors (as many of them already do) and States.

113 Osula & Rõigas (2018).

- Issues related to ensuring TSC security and integrity can be addressed through the (T)CBM toolkit as a specific component of critical infrastructure protection – a major part of the OSCE CBMs' scope.
- The set of cybersecurity (T)CBMs, including those adopted by the OSCE,[114] should be explored in detail to assess its applicability to advancing intergovernmental cooperation on addressing ICT-driven risks to TSCs.

GAP 8: OVERALL LOW LEVEL OF MATURITY OF NATIONAL FRAMEWORKS AND INITIATIVES TO ENSURE SECURITY AND INTEGRITY OF TSCS.

- As the overview of governmental responses in Section 4.3 illustrates, the majority of state-of-the-art responses at the national level to address ICT-driven risks to TSCs are concentrated within a limited number of States. The remaining picture demonstrates a much lower level of maturity in strategic, policy and regulatory responses to such challenges. Policy and regulatory gaps include:
  - Lack of strategic vision and goal-setting among regulators with regard to the technological transformation of the global supply chain and its impact at the national level, as well as to responses to associated security risks.
  - Lack of government-wide coordination of policymaking, regulatory measures and cooperation with industry and the technology community on supply chain security and integrity issues. In many cases, the regulatory activities are diffused between various structures, agencies and departments.
  - Lack of demand for – and resulting supply of – support from industry, technology and policy expert communities to governments' responses to ICT-driven challenges to supply chains.

114 OSCE (2012)

RECOMMENDATIONS TO ADVANCE OPERATIONALIZATION OF NORMATIVE INITIATIVES

Based on the analysis of the findings presented in this report, a number of recommendations can be made for further discussion with relevant stakeholders. Several notes are applicable to these recommendations and should be considered by the readers of this report:

- The recommendations are designed to address the gaps identified in Chapter 6.
- The recommendations are intended to spark discussion among policy makers, diplomats and other national experts involved in norm-developing efforts as well as industry, the wider technology community and other stakeholder groups.
- The recommendations are addressed to States, to multi-stakeholder fora, and to the United Nations as principal actors in charge of different processes related to cybersecurity norms.
- The recommendations are not intended to cover the whole spectrum of responses and solutions to ICT-driven risks to TSCs; they address these issues only in the context of the operationalization of international norms and norm-developing initiatives.

The following recommendations are made in this report:

1. Align the scope of proposed norms with a comprehensive SCRM approach and industry practices.
2. Strengthen coordination and synergy among multi-stakeholder norm-developing initiatives and promote unified and interoperable minimum requirements for technology suppliers.
3. Harmonize national processes for management of transnational technology vendors.
4. Consider establishing a dedicated platform to support United Nations-led processes in engaging with industry, the technology community and other multi-stakeholder groups and initiatives active in the supply chain security and integrity field.
5. Increase focus on capacity-building efforts.
6. Assess and identify opportunities for using the (T)CBM toolkit to ensure the security and integrity of TSCs.

7. Strengthen the institutional, strategic and policy coordination of efforts to address ICT-driven challenges to TSCs at a national level.

Each recommendation is further described in the following sections.

RECOMMENDATION 1: ALIGN THE SCOPE OF PROPOSED NORMS WITH A COMPREHENSIVE SCRM APPROACH AND INDUSTRY PRACTICES (ADDRESSES GAP 1 AND GAP 2)

Addressed to: United Nations GGE and United Nations OEWG.

As part of the discussions within the GGE, and leveraging the mandate of the OEWG to further develop norms, rules and principles, specific actions could include:

- Expanding the focus of (new or adopted) norms to address the whole continuum of ICT-driven risks and aligning the substance of proposed norms with comprehensive (end-to-end) SCRM approaches used by industry and the private sector technology community.
- Ensuring a better balance between 'negative' and 'positive' norms, taking into account the fundamental nature of technological, legal and other challenges that negative norms related to supply chains face (attribution in cyberspace, lack of instruments for effective verification and monitoring of compliance, etc.).

RECOMMENDATION 2: STRENGTHEN COORDINATION AND SYNERGY AMONG MULTI-STAKEHOLDER NORM-DEVELOPING INITIATIVES AND PROMOTE UNIFIED AND INTEROPERABLE MINIMUM REQUIREMENTS FOR TECHNOLOGY SUPPLIERS (ADDRESSES GAP 3)

Addressed to: Multi-stakeholder norm-developing initiatives and their contributors (States, industry, technology community).

Specific actions could include:

- Exploring opportunities for ensuring structured and systematic communication flow and information-sharing among multi-stakeholder norm-developing processes addressing global supply chain issues in the ICT context (e.g. Digital Geneva Convention, Cybersecurity Tech Accord, Charter of Trust, Paris Call).

- Launching a process for discussion and elaboration of a unified, or at least harmonized and interoperable, set of minimum security and certification requirements shared, supported and promoted jointly by major multi-stakeholder fora. Elements might include:
  - Common set of applicable best practices or codes of conduct among major technology vendors aimed at mitigating risk to the security and integrity of global supply chains.
  - Common set of security standardization and certification requirements for technology suppliers. One good example is the set of security requirements developed by Siemens as part of its Charter of Trust initiative.
  - Common framework for third-party risk assessment.
  - Common set of technical tools to ensure security and integrity along global TSCs (e.g. a system of digital identifiers for ensuring end-to-end traceability throughout supply chains).

RECOMMENDATION 3: HARMONIZE NATIONAL PROCESSES FOR MANAGEMENT OF TRANSNATIONAL TECHNOLOGY VENDORS (ADDRESSES GAP 4)

Addressed to: Member States.

- Explore the opportunities for coordination and harmonization across States of national approaches and processes for the management of transnational technology vendors to make them more transparent and aligned with global SCRM and vendor security assessment standards.

RECOMMENDATION 4: CONSIDER ESTABLISHING A DEDICATED PLATFORM TO SUPPORT UNITED NATIONS-LED PROCESSES IN ENGAGING WITH RELEVANT MULTI-STAKEHOLDER GROUPS AND INITIATIVES ACTIVE IN THE SUPPLY CHAIN SECURITY AND INTEGRITY FIELD (ADDRESSES GAP 5)

Addressed to: The United Nations.

- Within the mandate of the OEWG to establish regular institutional dialogue with broad participation, including of the private sector, consider establishing a dedicated platform (e.g. committee, task force) to support the operationalization of the international cybersecurity norms related to the integrity and security of supply chains. Such a platform, with a focus on supply chain issues, could conduct its activities on an ongoing basis, aggregating information, inputs and initiatives from industry, the technology community and other stakeholders and relaying its feedback to relevant United Nations-led processes. Some inputs that such a framework could provide to the GGE/OEWG and their participants may include:
  - Updates on and in-depth insights into the dynamics of the global cyber threat landscape with regard to global TSCs and other relevant subject areas.
  - Updates from the standardization community on developments in related areas (standardization of SCRM and security assurance, etc.).
  - Best practices and approaches of global technology vendors to mitigate ICT-driven risks to supply chain security and integrity.
  - Updates, proposals and general exchange of information between United Nations-led processes and multi-stakeholder initiatives addressing the security and integrity of global supply chains.
- The proposed platform is not supposed to counterbalance or substitute the intergovernmental cyber norm-developing processes, but rather provide necessary support to them in areas in which the private sector has an inherent primary role in the implementation of proposed norms. Ensuring the security and integrity of supply chains could be a flagship area of activity for such an initiative owing to its global, multi-stakeholder and technical nature.

RECOMMENDATION 5: INCREASE FOCUS ON CAPACITY-BUILDING EFFORTS (ADDRESSES GAP 6)

Addressed to: The United Nations, regional IGOs and Member States.

- To States:
  - Conduct a nationwide capability assessment focused on the mitigation of ICT-driven risks to supply chains. This could be conducted independently by each State through the use of a (self)-assessment tool for cyber-SCRM or with external support (e.g. another State, a regional organization, an independent third party) with a view to identifying gaps and capacity building needs.
- To regional IGOs:
  - Conduct a region-wide assessment of information and risk awareness, map capacity levels and capacity gaps in cyber-SCRM across Member States, and develop targeted training interventions accordingly.
  - Explore opportunities for creating resource centres or data hubs that would be mandated with aggregating useful information and resources, recommendations and technical tools from Member States and vendors to address ICT-driven risks to TSCs.
- To the State-led multilateral processes within the United Nations fora:
  - Explore opportunities for using the existing United Nations digital capacity-building frameworks, platforms and resources for aggregating useful information, self-assessment tools and other instruments to address and mitigate ICT-driven risks to supply chains (e.g. the Digital Blue Helmets initiative, [115] the capacity-building pillar of the Global Programme on Cybercrime by the United Nations Office on Drugs and Crime,[116] Pillar 4 of the Global Cybersecurity Agenda by the International Telecommunication Union (ITU) [117]). Aim available information and resources at various segments of the target audience: States and public sector organizations, large transnational vendors, and SMEs.

115 OICT (2019).
116 UNODC (n.d.).
117 ITU (n.d.).

- Encourage the use of the United Nations capacity-building resources (e.g. publications, portals and databases by the United Nations Office for Disarmament Affairs, UNIDIR and ITU) as an additional tool providing information and support to participants of United Nations-led intergovernmental discussions on norms addressing the security and integrity of TSCs.
- Consider including measures to ensure the security and integrity of TSCs in the scope of relevant global and regional surveys, rankings and assessments of Member States conducted by United Nations bodies (e.g. the Global Cybersecurity Index by the ITU).

RECOMMENDATION 6: ASSESS AND IDENTIFY OPPORTUNITIES FOR USING THE (T)CBM TOOLKIT TO ENSURE THE SECURITY AND INTEGRITY OF TSCS (ADDRESSES GAP 7)

Addressed to: The United Nations, regional IGOs and Member States.

- To the United Nations and regional IGOs:
  - Conduct a multi-stakeholder discussion on the applicability of (T)CBMs to advancing intergovernmental cooperation on mitigating ICT-driven risks to supply chains.
  - As part of the OEWG workings, investigate the need to expand the list of adopted cybersecurity (T)CBMs with measures specifically addressing the mitigation of cyber risks to TSCs or to formulate a contextual interpretation of already adopted (T)CBMs to reflect supply chain-specific issues.
- To Member States:
  - Sharing information, potentially on a unilateral basis, with other States or IGOs on ICT-driven threats to supply chains, incidents affecting public and private sectors, and detailed national approaches and best practices related to ensuring the security and integrity of TSCs.
  - Establishing bilateral trust and transparency measures with other States, such as the exchange of information on supply chain cybersecurity threats, risks and vulnerability vectors, and approaches to their mitigation.
  - Establishing bilateral technical measures to prevent and mitigate significant incidents caused by malicious activities in the global supply chain (e.g. use of a shared system of digital identifiers to ensure traceability along TSCs and identify potential points of compromise).

RECOMMENDATION 7: STRENGTHEN THE INSTITUTIONAL, STRATEGIC AND POLICY COORDINATION OF EFFORTS TO ADDRESS ICT-DRIVEN CHALLENGES TO TSCS AT A NATIONAL LEVEL (ADDRESSES GAP 8)

Addressed to: Member States.

- This recommendation has national scope and focuses on the need for improved coordination of States' efforts to mitigate ICT-driven challenges to supply chains at a domestic level. Recommended courses of actions include:
  - Conduct an assessment of national strategic, policy and regulatory frameworks and instruments intended to mitigate security challenges to supply chains.
    - If the coordination of policy development and regulatory efforts to mitigate cyber risks to supply chains cannot be delegated to a single government agency (as part of the functions of a national cybersecurity centre, or by establishing a dedicated body), consider establishing interministerial committees (or equivalent processes). Some references to international best practices might include the UK CPNI and NCSC, the coordination of a broader Defense Industrial Base network of suppliers by the Office of the Under Secretary of Defense for Acquisition and Sustainment in the United States, and the National Supply Chain Security Center initiative, recently proposed in the draft MICROCHIPS Act[118] in the United States.
  - Consider developing and adopting a policy or strategy document specifically addressing risks related to TSCs, including ICT-driven risks, and identifying major vectors, milestones and objectives of governments' efforts to address these risks.
  - Explore the opportunities for launching an institutional vehicle for multi-stakeholder collaboration on the mitigation of security risks and challenges to TSCs at a national level. Formats might include public–private partnerships, multi-stakeholder working groups under the government or sector-specific regulators, industry councils and associations, and so on.

118 Paganini (2019).

REFERENCE LIST

115th US Congress (2017-2018). 2017. *National Defense Authorization Act for Fiscal Year 2018*. As of 10 November 2019: https://www.congress.gov/bill/115th-congress/senate-bill/1519/text

3rd Generation Partnership Project (3GPP). 2019. 'About 3GPP'. As of 10 November 2019: https://www.3gpp.org/about-3gpp

Apple Inc. 2019. 'Supplier List'. As of 10 November 2019: https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf

BairesDev. 2019. 'Software Outsourcing Trends'. As of 10 November 2019: https://www.bairesdev.com/insights/software-outsourcing-trends

Bartol, Nadya. 2011. 'ICT SCRM – ISO Standards Update'. US National Institute of Standards and Technology. As of 10 November 2019: https://www.nist.gov/document-5893

Bhargava, Vishal, Raman Chander, José R Favilla, Wilco Kaijim & Spencer Lin. 2019. *Engineering and Construction Digital Supply Chains - How Leaders Are Increasing Visibility and Insight*. IBM. As of 10 November 2019: https://www.ibm.com/downloads/cas/GJOMQOWL

Boyens, Jon, Celia Paulsen, Rama Moorthy & Nadya Bartol. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* NIST Special Publication 800-161. US National Institute of Standards and Technology. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Centre for the Protection of National Infrastructure (CPNI). 2019. 'Supply Chain'. As of 10 November 2019: https://www.cpni.gov.uk/supply-chain

Check Point Research. 2019. *Cyber Attack Trends: 2019 Mid-Year Report.* Check Point Software Technologies Ltd. As of 10 November 2019: https://www.checkpoint.com/downloads/resources/cyber-attack-trends-mid-year-report-2019.pdf

Cisco. 2018. *Cisco 2018 Annual Cybersecurity Report*. As of 10 November 2019: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Co-Chairs of ANSI's JTC/CS1-ICT SCRM AdHoc Working Group. 2017. 'Contribution to the NIST RFI on Developing a Framework to Improve Critical Infrastructure Cybersecurity'. US National Institute of Standards and Technology. As of 10 November 2019: https://www.nist.gov/system/files/documents/2017/06/06/040813_cs1_ict_scrm_ad_hoc.pdf

Committee on National Security Systems. 2015. Committee on National Security Systems (CNSS) Glossary. CNSSI No. 4009, 5 April 2015. BAI Information Security / RMF Resource Center. As of 10 November 2019: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Computaris. 2016. 'Software Development Outsourcing in Europe: Trends and Figures'. As of 10 November 2019: http://www.computaris.com/wp-content/uploads/2016/09/Market-research_Software-development-outsourcing.pdf

CrowdStrike. 2018. 'Securing the Supply Chain'. As of 10 November 2019: https://www.crowdstrike.com/resources/wp-content/brochures/pr/CrowdStrike-Security-Supply-Chain.pdf

Cybersecurity and Infrastructure Security Agency (CISA). 2019. *Overview of Risks Introduced by 5G Adoption in the United States*. US Department of Homeland Security. As of 10 November 2019: https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf

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

Davidson, Don. 2014. 'Supply Chain Risk Management (SCRM): Managing Enterprise Risk when Outsourcing'. US Department of Defense. As of 10 November 2019: https://supplychain.gsfc.nasa.gov/sites/supplychain/files/docs/2014/D.%20Davidson%20-%20SC2014.pptx.pdf

Defense Business Board. 2017. *Logistics as a Competitive War Fighting Advantage*. As of 10 November 2019: https://dbb.defense.gov/Portals/35/Documents/Reports/2017/DBB%2017-03%20Logistics%20Study%2020170509%20FINAL.pdf

Designveloper. 2019. 'Why You Should Partner with a Vietnam Software Outsourcing Company?'. As of 10 November 2019: https://www.designveloper.com/partner-vietnam-software-outsourcing-company

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. *Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks*, EU Document C(2019) 2335 final. As of 10 November 2019: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks

———. 2019c. 'Key Players in European Standardisation'. As of 10 November 2019: https://ec.europa.eu/growth/single-market/european-standards/key-players_en

———. 2019d. '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 Cybersecurity (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

Evermann, Annelie. 2014. *The ICT Sector in the Spotlight - Leverage of Public Procurement Decisions on Working Conditions in the Supply Chain*. Electronics Watch Consortium. As of 10 November 2019: http://electronicswatch.org/the-ict-sector-in-the-spotlight_723519.pdf

Feinstein, Dianne. 2019. 'Feinstein Statement on 5G National Security Concerns'. United States Senator for California Dianne Feinstein, 14 May. As of 10 November 2019: https://www.feinstein.senate.gov/public/index.cfm/press-releases?id=FDC03D62-C440-40DB-9568-91E1103C8B0F

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

Google. 2018. *Responsible Supply Chain Report 2018*. As of 10 November 2019: https://storage.googleapis.com/gweb-sustainability.appspot.com/RSC/Google_2018-RSC-Report.pdf

Group of Seven (G7). 2018. *G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*. Department of Finance Canada. As of 10 November 2019: https://www.fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf

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

Howard, Michael, Jon Pincus & Jeannette M. Wing. 2003. 'Measuring Relative Attack Surfaces'. Colorado State University. As of 10 November 2019: https://www.cs.colostate.edu/~malaiya/635/09/Howard03.pdf

Huawei. 2019. 'Supply Chain Responsibilities'. As of 10 November 2019: https://www.huawei.com/en/about-huawei/sustainability/win-win-development/develop_supplychain

Huawei Cyber Security Evaluation Centre Oversight Board. 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

Hurel, Louise Marie, & Luisa Cruz Lobato. 2018. 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs'. *Journal of Cyber Policy* 3(1): 61–76. doi:10.1080/23738871.2018.1467942

IBM. 2017a. *Supply Chain - 2017 Corporate Responsibility Report*. As of 10 November 2019: https://www.ibm.com/procurement/openPdf?file=IBM_2017_CRR_SupplyChain.pdf

———. 2017b. *The Future Supply Chain - The Challenges and Technologies Shaping the Future Supply Chain.* White paper. Watson Customer Engagement. As of 10 November 2019: https://www.ibm.com/downloads/cas/DZKEVME3

International Organization for Standardization (ISO). 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

———. 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

———. 2019. *ISO/IEC JTC 1/SC 27: Information Security, Cybersecurity and Privacy Protection*. As of 10 November 2019: https://www.iso.org/committee/45306.html

International Telecommunication Union (ITU). n.d. 'Global Cybersecurity Agenda (GCA)'. As of 10 November 2019: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Joint Committee on the National Security Strategy. 2018. *Cyber Security of the UK's Critical National Infrastructure - Third Report of Session 2017-19. HL Paper 222, HC 1708*. House of Lords, House of Commons. As of 10 November 2019: http://www.dirittoepoliticadeitrasporti.it/wp-content/uploads/2018/12/House-of-Lords-and-House-of-Commons-Cyber-Security-of-the-UKs-Critical-National-Infrastructure-Nov-2018.pdf

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

Kavanagh, Camino. 2019. Stemming the Exploitation of ICT Threats and Vulnerabilities – An Overview of Current Trends, Enabling Dynamics and Private Sector Responses. United Nations Institute for Disarmament Research. As of 10 November 2019: https://unidir.org/files/publications/pdfs/stemming-the-exploitation-of-ict-threats-and-vulnerabilities-en-805.pdf

Khan, Muhammad Arsalan. 2018. 'Globalization of Logistics and Supply Chain Management', conference paper, *Proceedings International Conference on Industrial Engineering and Operations Management*, Kuala Lumpur, 8–10 March 2016. As of 10 November 2019: https://www.researchgate.net/publication/329238875_Globalization_of_Logistics_and_Supply_Chain_Management

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

Martinsson, Johanna. 2011. *Global Norms: Creation, Diffusion, and Limits*. The World Bank, Communication for Governance and Accountability Program. As of 10 November 2019: http://siteresources.worldbank.org/EXTGOVACC/Resources/FinalGlobalNormsv1.pdf

McKinsey & Company. 2016. 'Supply Chain 4.0 – The Next-Generation Digital Supply Chain'. As of 10 November 2019: https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-40--the-next-generation-digital-supply-chain

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

———. 2018a. '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

———. 2018b. 'Attack inception: Compromised supply chain within a supply chain poses new risks'. Microsoft Defender ATP Research Team, July 28. 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

———. 2019. 'Supplier Privacy & Assurance Standards'. As of 10 November 2019: https://www.microsoft.com/en-us/procurement/sspa?activetab=pivot%3aprimaryr3

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

———. 2019b. 'Connected Industries'. As of 10 November 2019: https://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html

National Cyber Security Centre (NCSC). 2019. 'Protect Your Organisation against Cyber Attack'. As of 10 November 2019: https://www.cyberessentials.ncsc.gov.uk

Newman, Lily Hay. 2017. 'Hacker Lexicon: What Is an Attack Surface?' Wired, 12 March, 08:00 ET. As of 10 November 2019: https://www.wired.com/2017/03/hacker-lexicon-attack-surface

Nissen, Chris, John Gronager, Robert Metzger & Harvey Rishikof. 2018. *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 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 Press Secretary. 2017. 'DHS Statement on the Issuance of Binding Operational Directive 17-01'. US Department of Homeland Security, 13 September. As of 10 November 2019: https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

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

Office of the Under Secretary of Defense for Acquisition and Sustainment, & Office of the Deputy Assistant Secretary of Defense for Industrial Policy. 2018. *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States.* US Department of Defense. As of 10 November 2019: https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

Organisation for Economic Co-operation and Development (OECD). 2018. *Global Outlook on Financing for Sustainable Development 2019: Time to Face the Challenge*. Paris: OECD Publishing. doi:10.1787/9789264307995-en

Organization for Security and Co-operation in Europe (OSCE). 2012. *OSCE Guide on Non-Military Confidence-Building Measures (CBMs)*. As of 10 November 2019: https://www.osce.org/secretariat/91082?download=true

Osula, Anna-Maria, & Henry Rõigas, eds. 2016. *International Cyber Norms Legal, Policy and Industry Perspectives*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications. As of 10 November 2019: https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf

Paganini, Pierluigi. 2019. 'MICROCHIPS Act Aims at Improving Tech Supply Chain'. SecurityAffairs, 1 August. As of 10 November 2019: https://securityaffairs.co/wordpress/89224/laws-and-regulations/microchips-supply-chain-security.html

Parliamentary Office of Science and Technology. 2017. *Cyber Security of UK Infrastructure.* Postnote Number 554, May 2017. Houses of Parliament. As of 10 November 2019: http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf

Paulsen, Celia. 2013. 'ICT Supply Chain Risk Management'. US National Institute of Standards and Technology. As of 10 November 2019: https://csrc.nist.gov/CSRC/media//Projects/Forum/documents/june2013_presentations/forum_june2013_cpaulsen.pdf

PricewaterhouseCoopers (PwC). 2015. *Disclose In the Spotlight: New Business Models*. Issue 2, 2015. As of 10 November 2019: https://disclose.pwc.ch/22/media/pdf/pwc_disclose_1502_e.pdf

———. 2016. *Industry 4.0: Building the Digital Enterprise.* As of 10 November 2019: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

PRNewswire. 2018. 'The Global Supply Chain Management Software Market Size Is Expected to Reach $22.7 Billion by 2024, Rising at a Market Growth of 12.1% CAGR during the Forecast Period'. PRNewswire.com, 22 August, 09:08 ET. As of 10 November 2019: https://www.prnewswire.com/news-releases/the-global-supply-chain-management-software-market-size-is-expected-to-reach-22-7-billion-by-2024--rising-at-a-market-growth-of-12-1-cagr-during-the-forecast-period-300700907.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

ResearchMoz. 2019. 'Global Supply Chain Management Software Market Growth, Forecast and Value Chain 2019-2025'. Commerce Gazette, 23 September. As of 10 November 2019: https://commercegazette.com/2019/09/23/supply-chain-management-software-market-growth-forecast-and-value-chain-2019-2025

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

Samsung. 2019. 'Responsible Management of Supply Chain'. As of 10 November 2019: https://www.samsung.com/us/aboutsamsung/sustainability/supply-chain

SAP. 2019. 'Digital Supply Chain'. As of 10 November 2019: https://www.sap.com/products/digital-supply-chain.html

Siemens AG. 2019. 'Siemens Establishes Binding Cybersecurity Requirements for Suppliers'. Press Release. Siemens AG, 15 February. As of 10 November 2019: https://press.siemens.com/global/en/pressrelease/siemens-establishes-binding-cybersecurity-requirements-suppliers?content[]=Corp

Stockton, Paul. 2018. Securing Critical Supply Chains – Strategic Opportunities for the Cyber Product International Certification (CPIC™) 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

Symantec. 2019. *ISTR Internet Security Threat Report, Vol. 24*. As of 10 November 2019: https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf?aid=elq_19296

The Open Group. 2014. *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?_ga=2.34603688.806857558.1575029424-72192277.1567443766

Trustworthy Software Foundation. 2019. 'TS Framework'. As of 10 November 2019: http://tsfdn.org/ts-framework

United Nations General Assembly (UNGA). 1999. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/53/70, 4 January 1999. As of 10 November 2019: https://digitallibrary.un.org/record/1655670

———. 2013. Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international securityD, UN document A/68/98, 24 June 2013. As of 10 November 2019: https://digitallibrary.un.org/record/753055

———. 2015. '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

———. 2018. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly on 5 December 2018. UN document A/RES/73/27, 11 December 2018. As of 10 November 2019: https://undocs.org/A/RES/73/27

United Nations Office for Disarmament Affairs (UNODA). 2019a. 'China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security'. As of 10 November 2019: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf

———. 2019b. 'Developments in the Field of Information and Telecommunications in the Context of International Security'. As of 10 November 2019: https://www.un.org/disarmament/ict-security

United Nations Office of Information and Communications Technology (OICT). 2019. 'Digital Blue Helmets'. As of 10 November 2019: https://unite.un.org/digitalbluehelmets

United Nations Office on Drugs and Crime (UNODC). n.d. 'Global Programme on Cybercrime'. As of 10 November 2019: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

UN Web TV. 2019. '(1st Meeting) Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security'. UN Web TV, 9 September. As of 10 November 2019: http://webtv.un.org/search/1st-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security/6084740970001/?term=open%20ended%20information%20group&lan=English&cat=Meetings%2FEvents&sort=date&page=2

US Department of Defense (DoD). 2018. 'Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)'. Department of Defense Instruction Number 5200.44, 5 November 2012, incorporating Change 3, 15 October, 2018. As of 10 November 2019: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=2018-11-08-075800-903

US Department of Defense (DoD), US General Services Administration (GSA) & US National Aeronautics and Space Administration (NASA). 2019. *Federal Acquisition Regulation: Use of Products and Services of Kaspersky Lab.* Federal Register, 10 September. As of 10 November 2019: https://www.federalregister.gov/documents/2019/09/10/2019-19360/federal-acquisition-regulation-use-of-products-and-services-of-kaspersky-lab

US National Institute of Standards and Technology (NIST). 2018a. 'Cybersecurity Framework. Industry Impacts'. As of 10 November 2019: https://www.nist.gov/industry-impacts/cybersecurity

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

———. 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

US National Institute of Standards and Technology (US NIST) Computer Security Resource Center (CSRC). n.d.a. 'Glossary. Backdoor'. As of 10 November 2019: https://csrc.nist.gov/glossary/term/backdoor

———. n.d.b. 'Glossary. Logic Bomb'. As of 10 November 2019: https://csrc.nist.gov/glossary/term/logic-bomb———. 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

———. 2019a. *Best Practices in Cyber Supply Chain Risk Management - Cisco, Managing Supply Chain Risks End-to-End*. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Cisco_071515.pdf

———. 2019b. Best Practices in Cyber Supply Chain Risk Management – DuPont Crop Protection, Operating Disciplines for Supply Chain Sustainability, Risk Management and Resilience. As of 10 November 2019:

https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_DuPont_071315.pdf

———. 2019c. *Best Practices in Cyber Supply Chain Risk Management - FireEye, Supply Chain Risk Management.* As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_FireEye_081415.pdf

———. 2019d. Best Practices in Cyber Supply Chain Risk Management – Fujitsu Network Communications, Managing Supply Chain Risks in Optical and Wireless Networking. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Fujitsu_091615.pdf

———. 2019e. *Best Practices in Cyber Supply Chain Risk Management - Intel Corporation, Managing Risk End-to-End in Intel's Supply Chain*. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Intel_100715.pdf

———. 2019f. *Best Practices in Cyber Supply Chain Risk Management - Juniper Networks, Ensuring a Remarkable Customer Experience.* As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Juniper_081415.pdf

———. 2019g. Best Practices in Cyber Supply Chain Risk Management – Northrop Grumman Corporation, Trusted, Innovative, World-Class Supply Chain. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Northup_081615.pdf

———. 2019h. 'Cyber 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

US White House. 2018. *National Cyber Strategy of the United States of America*. As of 10 November 2019: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

———. 2019a. *The Comprehensive National Cybersecurity Initiative.* As of 10 November 2019: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

———. 2019b. 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain'. Whitehouse.gov, 15 May. As of 10 November 2019: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain

Weatherford, Mark. 2018. 'Cybersecurity: A Growing Risk for Supply Chain Risk Management'. US National Aeronautics and Space Administration (NASA) website. As of 10 November 2019: https://supplychain.gsfc.nasa.gov/sites/supplychain/files/docs/2018/weatherford-SC2018.pdf

Wieland, Andreas, & Carl Marcus Wallenburg. 2011. *Supply-Chain-Management in stürmischen Zeiten*. Berlin: Universitätsverlag der TU.

World Bank & World Trade Organization (WTO). 2019. *Global Value Chain Development Report 2019 - Technological Innovation, Supply Chain Trade, and Workers in a Globalized World*. As of 10 November 2019: http://documents.worldbank.org/curated/en/384161555079173489/Global-Value-Chain-Development-Report-2019-Technological-Innovation-Supply-Chain-Trade-and-Workers-in-a-Globalized-World

Wright, Jeremy. 2019. 'Jeremy Wright's Oral Statement on the Telecoms Supply Chain Review'. Gov.uk, 22 July. As of 10 November 2019: https://www.gov.uk/government/speeches/jeremy-wrights-oral-statement-on-the-telecoms-supply-chain-review


40
UNIDIR
UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH