PARIS CALL

FOR TRUST AND SECURITY IN CYBERSPACE

11 • 12 • 2018

Paris Call for Trust and Security in Cyberspace

Working Group (WG) 6: Bringing concrete tools to the Paris Call community

REPORT

Securing ICT supply chains

Cigref SUCCEED WITH DIGITAL

kaspersky

GEODE

EXECUTIVE SUMMARY

Working Group 6 (*further* – WG6) was created within the Paris Call for Trust and Security in Cyberspace to bring concrete tools to the Paris Call community. The co-chairs – Cigref and Kaspersky, with the support by GEODE and more than 20 other members representing different stakeholder groups and regions – have discussed the policy gaps and implementation challenges to ensuring ICT supply chain security.

WG6's main objective is to **bring knowledge to the Paris Call community and beyond, on the implementation of existing recommendations produced by the Organisation Economic Cooperation and Development (OECD), as well as share practical actionable steps stakeholder groups can take for stronger ICT supply chain security through the matrix developed.** While there are already many existing ICT supply chain security frameworks (which our mapping reveals), we hope to provide concrete knowledge to the Paris Call community and beyond to enable it to be better informed on how and with which tools they could enhance their ICT supply chain security.

Throughout 2021, WG6 focused on several step-by-step workstreams to continuously elaborate on this issue. As result, WG6 has conducted mapping of key existing frameworks related to ICT supply chain security, and the outcomes of the mapping can be used by both policy makers and industry to identify existing good practices, guidance, and partnerships where they could contribute and participate. The mapping also further informed the discussion on key factors leading to either success or failure in the implementation of security practices and requirements to provide stronger ICT supply chain security. In this regard, WG6 outlined possible incentives where they are presently still absent. Finally, to bring a concrete outcome to Paris Call supporters and beyond, WG6 has produced the matrix with practical, actionable steps to clearly highlight zones where different stakeholder groups have a role to play to collectively build stronger ICT supply chain security. The matrix has also been used as a basis for preparing targeted recommendations.

At the end of this report, we provide key conclusions and recommendations to support further discussions in the Paris Call community and beyond. They are summarized as follows:

All actors have a role to play toward stronger ICT supply chain security. If some actors do not make their contribution, there will be higher security and safety risks for all across supply chains. To identify for actors their possible contribution, we have prepared the matrix with suggestions on pragmatic and real actions to make a positive security impact.

Build on what already exists: there are already many existing ICT supply chain security frameworks, and actors can participate or use their outcomes for making both individual and collective impacts for stronger ICT supply chain security.

However, certain areas require further action: **ensuring harmonization across emerging national regulatory and industry approaches; creating incentives for security-focused behavior on both the supply and demand side**; and **further enhancing ICT supply chain transparency by both the public and private sector**.

Ensuring the security of ICT products and services is a continuous effort, throughout the deployment lifecycle, to protect customers and end-users, that's why certifications, conformity assessments and labels should not be an end state.

Interoperability, harmonization and reciprocity on national and international levels are key in making emerging national regulatory approaches work and produce a positive economic and security impact.

In this regard, we **call for strengthening cooperation across all levels and sectors** – between digital security experts and ICT manufacturers to implement security-by-design practices; between the private and public sector broadly to develop effective risk-based regulatory approaches; and between states and international organizations – to enhance interoperability and harmonization in present and future regulation of ICT supply chain.

ACKNOWLEDGMENTS

Working Group 6 (*further* – WG6) is co-chaired by Cigref and Kaspersky, with the support by GEODE.

The steering committee is composed of:

- Cigref: Arnaud COUSTILLIÈRE, Paris Call's Cigref Representative; Clara MORLIÈRE, Senior Mission Officer;
- Kaspersky: Anastasiya KAZAKOVA, Senior Public Affairs Manager, Cyber Diplomacy; Arnaud DECHOUX, Public Affairs Manager Europe;
- GEODE: Dr. Aude GERY, Post-doctoral researcher.

WG6 included several organizations and individuals who supported the international collective work from March to November 2021.

The Steering Committee is honored to have such incredible expert support, and wishes to thank all experts participating in WG6 and contributing to its work by providing their valuable feedback on outcomes of the all workstreams and earlier versions of this final report, and in particular (in alphabetical order):

- Imad AAD, Center for Digital Trust (c4dt.org), EPFL
- Nele ACHTEN, Center for Security Studies (CSS), ETH Zurich
- Laurent BERNAT, Organisation for Economic Co-operation and Development (OECD)
- Gérôme BILLOIS, Wavestone
- Anna COLLARD, KnowBe4 Africa Olivier Clément, Enedis
- Efrat DASKAL, DiploFoundation
- Brendan DUNPHY, CyberNB | CIPnet
- Jonas GRÄTZ, Federal Department of Foreign Affairs (FDFA), Switzerland
- Tyson JOHNSON, CyberNB | CIPnet
- Andreas KUEHN, Observer Research Foundation (ORF) America
- May-Ann LIM, Asia Cloud Computing Association
- Marguerite QUICHAUD, Wavestone
- Vladimir RADUNOVIĆ, DiploFoundation
- Ghislain de SALINS, Organisation for Economic Co-operation and Development (OECD)

This report is a consolidation of multiple views and positions from the participants of the working group, proposed by the co-chairs.

The collective work presented in this report does not reflect the position of any organization and/or expert listed here.

GLOSSARY

CVD : Coordinated Vulnerability Disclosure

VEP: Vulnerability Equities Process

EOL : End Of Life

ICT : Information and Communications Technology

OECD : Organisation for Economic Co-operation and Development

SMEs : Small and Medium-sized Enterprises

GCSC : Global Commission on the Stability of Cyberspace

GGE : Group of Governmental Experts

SBOM : Software Bill of Materials

OSCE : Organization for Security and Co-operation in Europe

OUTLINE

INTRODUCTION

Context

Information and communications technologies have been transforming our societies and economies, providing major opportunities for innovation, economic progress, cultural development and access to information. However, they also come with new risks: threat actors, and dangerous practices. Cyberattacks are growing in number and intensity, affecting more and more organizations – public or private, large or small – as well as individuals. They constitute a growing threat to our societies and economies and to international peace and security.

In this context, states have been discussing in various fora how to guarantee the security and stability of cyberspace. Many nations have recognized that international law applies in cyberspace [1] and promote norms of responsible state behavior and confidence-building measures.

However, dangerous practices and threats can come from both state and non-state actors in cyberspace. Cyberspace is run and managed by a large, diverse number of actors, and all actors, including the private sector, have a role to play and a responsibility to assume when it comes to adopting responsible behavior and finding solutions to the new cyberthreats. Multi-stakeholder cooperation among states, industry, academia and civil society, which is at the heart of the Paris Call for Trust and Security in Cyberspace, is essential to ensure the security and stability of cyberspace.

The Paris Call and working groups 'objectives

The Paris Call for Trust and Security in Cyberspace [2] (*further* – the Paris Call), launched by French President Emmanuel Macron in November 2018, promotes a multi-stakeholder approach to improve trust, security and stability in cyberspace in collaboration with states, local governments, private sector entities and civil society organizations. It has now become the largest multi-stakeholder initiative in the world on cybersecurity, with more than a thousand supporters from all sectors and regions. The Paris Call is organized around [3].

To keep growing and strengthening the Paris Call community, the French Minister for Europe and Foreign Affairs, Jean-Yves Le Drian, announced the [4] of six working groups at the third sitting of the Paris Peace Forum in November 2020.

These working groups were open to all interested supporters. They explore opportunities and tools to develop, deepen and strengthen the Paris Call community and facilitate information sharing, and exchange and promotion of good practices among the Paris Call's supporters.

Each working group is co-chaired by two or three supporters of the Call from different sectors and countries. Each has its own organization, meeting schedule and objectives, which are defined collectively among participants. Working groups present their results and deliverables at the Paris Peace Forum in November 2021.

The overarching goal of this group is to propose concrete tools to the supporters of the Paris Call to help them improve their cybersecurity level. Despite the efforts of cybersecurity actors and the adoption of best practices and standards, vulnerabilities and sources of insecurity remain widespread in cyberspace, and in line with the sixth principle of the Paris Call[1], the WG6's Steering Committee has decided to focus on the issue of ICT supply chain security and various actionable steps for stakeholder groups.

Our objectives

In the spirit of the Paris Call's principles and its multi-stakeholder nature, WG6 focuses on ICT supply chain security to address the following challenges:

1. **'Knowledge gap'**, i.e., lack of instrumental, practical guidance on existing good practices, policies, security baselines, and frameworks relating to ICT supply chain security;
2. **'Implementation gap'**, i.e., challenges arising due to the lack of implementation and application of those practices, policies and security baselines; and
3. **'Action gap'**, i.e., lack of clear understanding of capacities, capabilities and actionable steps for each stakeholder group (public sector, international organizations, ICT manufacturers, security providers, customers and end-users) in ensuring ICT supply chain security.

Thus, the core objective of WG6 is to raise awareness and provide analytical background information for policy makers and industry within the Paris Call community and beyond on ICT supply chain security through informing about where gaps exist, but also where and what each stakeholder group has a key role to play and how each could contribute to ensuring ICT supply chain security.

This objective is achieved through the following steps:

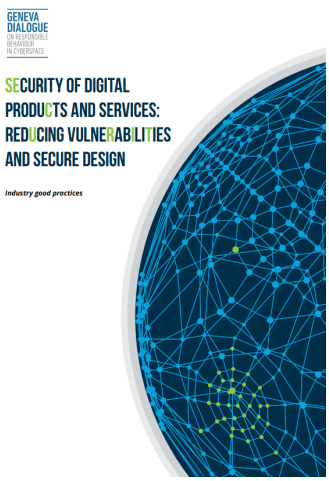
Our approach

The concept of ICT supply chain security: as our study will show, there is no single definition of the concept of ICT supply chain security. We thus intentionally apply the term 'ICT supply chain security' as an overarching definition comprising a set of related frameworks, practices, steps, measures, etc. relating to the security of the digital sector.

Building on what has been achieved so far: different stakeholders have already been working on the issue of ICT supply chain security. To conduct its work, WG6 thus decided to build on what has been achieved at other for a, such as the UN (within the Groups of Governmental

[1] The sixth principle of the Paris Call aims to strengthen the security of digital processes, products and services throughout their lifecycle and supply chain. More information is available at https://pariscall.international/en/principles.

Experts, and the Open-Ended Working Group on Cyber) [5] and the Geneva Dialogue on Responsible Behaviour in Cyberspace [6].



In particular, WG6 chose to use the OECD report on 'Enhancing the digital security of products' as a basis to conduct its work. Two main reasons motivated this choice:

- The importance of the role of the OECD on economic matters and its expertise to provide a thorough analysis on this issue from an economic policy perspective [7], as well as its ability to develop guidelines for OECD members, taking non-governmental stakeholders' views into account in its process; and
- The ongoing OECD's work on updating recommendations for the digital security of products, and thus their possible impact on and contribution to implementation of the principle six of the Paris Call on lifecycle security.

Therefore, WG6 took the six OECD High-level principles [8] to identify existing patterns and gaps in implementation of the ICT supply chain security-related frameworks and make concrete recommendations for each stakeholder group for stronger ICT supply chain security.

Our roadmap

To tackle the implementation issues to ensure ICT supply chain security, our work started with identifying frameworks focusing on ICT supply chain security, including the security of digital products. We then took the key findings and recommendations from OECD analytical work in this area [8], and split them into several actionable steps to provide a basis for conducting a mapping of the frameworks.

The mapping served as a foundation for identifying incentives as well as factors leading to failure or success in the implementation of those frameworks. The mapping also informed further discussion on the actionable steps for different stakeholder groups to ensure stronger ICT supply chain security.

WG6's work was thus split up into several step-by-step workstreams:

- **WORKSTREAM I:** Developing the mapping of existing frameworks relating to ICT supply chain security to identify what exists and where policy gaps are, if any.
- **WORKSTREAM II.** Identifying cases and factors leading to failure in implementation and application of the analyzed frameworks in the field of ICT supply chain security.
- **WORKSTREAM III.** Reflecting on the actionable steps within the roles that different stakeholder groups need to play in ensuring ICT supply chain security.
- **WORKSTREAM IV.** Producing a final report with key high-level targeted (depending on stakeholder groups) recommendations.

WORKSTREAM I: MAPPING OF EXISTING FRAMEWORKS

Goal of workstream I: Developing a mapping of frameworks relating to ICT supply chain security to identify what exists and where policy gaps are, if any. Thus, the outcomes of workstream I will help fill the 'knowledge gap' (1).

Additionally, as we analyze the existing frameworks in this field and see how they relate to the high-level principles developed by the OECD, we have started working on and filling the 'implementation gap' (2) to provide a better understanding of how those OECD high-level principles are already addressed with the existing efforts in the global community.[2]

The mapping can serve to raise awareness and provide analytical background information for policy makers and industry through developing a methodology for comparing existing frameworks in the field of ICT supply chain security and demonstrating how they interact and complement each other. The mapping completed can also be used by policy makers and industry in:

- Exploring the existing initiatives and approaches to addressing risks related to the ICT supply chain security;
- Developing mitigation strategies through learning and applying the recommendations and particular actions that the initiatives included in the mapping promote;
- Identifying any existing policy gaps for further actionable efforts in the global community.

Classification and analysis of the frameworks in the field of ICT supply chain security

The classification of the frameworks relating to ICT supply chain security (laws, standardization documents, conferences' outcome documents, etc.) is based on a combination of three criteria: type of document, status of document, and its origin.

It is critical to note that the frameworks identified below should not be understood as opposing categories, but rather considered and analyzed further in their linkages. Even within a single category, we may find very different types of documents that do not have the same normative value and thus should not be understood as the same.

Why is it important to distinguish between the different frameworks? They can have different purposes and can complement each other, but at the same time, their legal and political value and focus on target audiences will vary. Distinguishing between the different types of frameworks thus helps us understand where gaps might be and, therefore, where future action might be needed.

The analysis does not claim to be exhaustive and comprehensive. The list in Annex 1: ICT supply chain-related frameworks analyzed reflects the discussions within WG6 and the intentions of WG6 to provide diversity in the analysis of the frameworks. At the same time, given the growing interest of policy makers and industry in ICT supply chain security, further work might be considered to extend the scope of the mapping and identify additional frameworks that are not included in the 2021 work of WG6.

[2] Under 'global community' we understand a broad range of state and non-state stakeholders working in field of, and with matters relating to, ICT supply chain security.

Categories	Type of document	Status	Origin
Public policy	Laws, regulations, guidelines	Mandatory or voluntary	A public authority allowed to adopt laws or regulations, according to a state's constitutional system, as well as to publish guidelines of a voluntary nature
Standardization & labelling	Technical standards, specifications, voluntary certifications and labelling	Mandatory or voluntary	Elaborated and/or promoted by a public or private authority for third-parties to implement and follow, based on self-assessment or external third-party evaluation
Corporate & non-governmental	Internal policies and/or processes	Non-mandatory[3]	Elaborated and/or promoted by a company/group of companies or by a non-governmental organization or organizations for itself/themselves
Public-private	Collections of good practices, reports, statements	Non-mandatory	Elaborated and/or promoted by a group of states and non-state actors together
Intergovernmental	International legal or policy documents	Binding or non-binding	Elaborated and/or promoted by an international or regional organization or an informal group of States

Thus, we have analyzed thirteen public policy frameworks, six standardization and labelling frameworks, six corporate and non-governmental frameworks, three public-private frameworks, and seven intergovernmental frameworks. The detailed list is provided in ANNEX: ICT supply chain-related frameworks analyzed.

[3] Non-mandatory for external recipients, but they could be mandatory for internal purposes.

Comparing these frameworks to the six OECD high-level principles

Given the considerations listed earlier, WG6 chose to base its analysis on the OECD 2021 report on the Digital Security of Products [9] (*further* – the OECD report). This report identified concrete actions under each high-level principle, and we applied this approach for our methodology in conducting the mapping of the frameworks relating to ICT supply chain security.

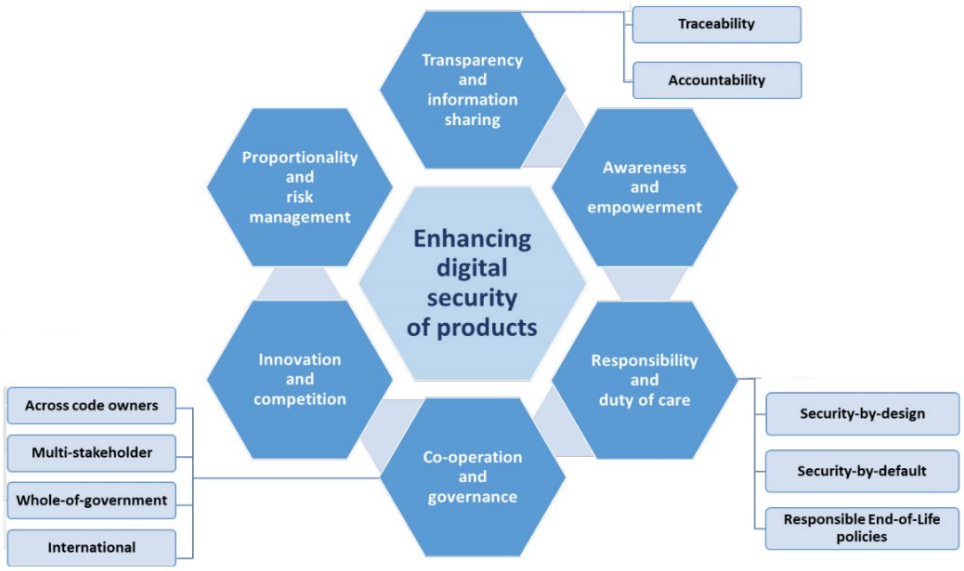


Figure 1. Overview of the six OECD high-level principles

Source: OECD.

As a result, we have a table showing the OECD high-level principles: transparency and information sharing; awareness and empowerment; responsibility and duty of care; co-operation and governance; innovation and competition; and proportionality and risk management. Within these high-level principles, we list twenty-five actions, following closely the OECD report:

OECD high-level principles	Actions
Transparency and information sharing	▪ A1: Increasing and providing transparency on product features for digital security ▪ A2: Increasing and providing transparency on processes and policies that are put in place by supply-side actors (e.g. end of life gap) ▪ A3: Increasing and providing transparency on the product's code ▪ A4: Increasing and providing transparency on traceability (list of code components, product's value chain, data processing) ▪ A5: Increasing and providing transparency on general trustworthiness (broader ecosystem: track-record of the organization for managing digital security, impact of applicable domestic laws etc.) ▪ A6: Increasing and providing transparency on third-party evaluation (including certification, labels, security audits)

OECD high-level principles	Actions
Awareness and empowerment	▪ A7: Promoting labels ▪ A8: Launching awareness-raising campaigns and/or developing guidelines and/or supporting educational programs for educating mainstream users about basic digital security "hygiene" ▪ A9: Promoting and engaging in capacity building and training programs for developing skills for small and medium enterprises (SMEs) ▪ A10: Providing 'effective consumer protection' - i.e. ensuring protection of privacy; dispute resolution mechanisms; protecting vulnerable and disadvantaged consumers; protecting consumers from hazards to their health and safety etc. ▪ A11: Empowering advanced users to adjust the level of digital security based on their own risk assessment (access and modify security settings; opting out from security defaults such as automatic updates; etc.)
Responsibility and duty of care	▪ A12: Adopting and/or implementing security-by-design requirements/standards/certification/conformity assessments ▪ A13: Adopting and/or implementing ex post mechanisms (e.g. insurance and liability law) and public procurement requirements ▪ A14: Adopting and/or implementing dynamic management of digital security (vulnerability management, CVD policies, vulnerability handling processes, bug bounty programs etc.) ▪ A15: Adopting and/or implementing responsible EOL policies ▪ A16: Ensuring the digital security of organizations (e.g. adhering to international standards such as ISO 31000) and national jurisdiction
Co-operation and governance	▪ A17: Increasing co-operation amongst code owners across the value chain (through facilitating security bulletins, procurement guidelines, applying unique digital identities for processes, products and organizations) ▪ A18: Promoting and engaging in multi-stakeholder cooperation which includes, but not limited to, security researchers (bug bounties, VD policies); competitors (through ISACs); CERTs; other relevant stakeholders (e.g. consumer associations) ▪ A19: Adopting and/or implementing the whole of government approach (i.e. involving all relevant government agencies and institutions in charge of horizontal and sectoral regulations) ▪ A20: Promoting and engaging in international co-operation
Innovation and competition	▪ A21: Promoting and/or engaging in research and development ▪ A22: Creating market incentives (e.g. through simplifying regulatory compliance or creating innovative policies such as regulatory sandboxes) ▪ A23: Encouraging and/or implementing voluntary frameworks to support competition

OECD high-level principles	Actions
Proportionality and risk management	▪ A24: Adopting and/or implementing risk-based multi-layered/tiered approaches ▪ A25: Adopting and/or developing proportionate measures and policies (through impact assessments or engaging industry's inputs)

Key insights from analyzing the mapping

The analysis of the mapping provides several insights:

1. **No commonly-used definition or description of what ICT supply chain security includes was found in the frameworks analyzed. ICT supply chain security is also approached by different stakeholder groups through different lenses, which signals different emphases and goals they pursue.**

We found that some frameworks provide definitions (e.g., the U.S. NIST Specification, or the ENISA Guidelines), while others do not. In addition, there are several variations used: 'cyber supply chain', 'supply chain', 'ICT supply chain', 'software supply chain', 'digital supply chain', and there is little knowledge on the exact differences among these notions or whether they can be used as synonyms. Most of the frameworks analyzed also apply language that could lead to adopting a broader interpretation of the terms, therefore raising interpretation issues and leaving some leeway for interpretation.

ICT supply chain security is approached in the frameworks analyzed in different ways:

- as a set of management practices for encouraging choosing trustworthy software products and ensuring digital security (in the context of national security and national economic policy conversations);
- as a set of product development and engineering practices with the focus on security-by-design and software lifecycle development practices (in the context of cybersecurity, network and information security and technical conversations);
- as a set of multilateral and multi-stakeholder practices (in the context of digital-cooperation-related conversations);
- as normative (promoting certain behavior) practices (in the context of international security conversations).

The variety of approaches and terminology used reflect different emphases and goals that stakeholder groups pursue in discussions on ICT supply chain security. Variations in terminology also occur because of states' varying approaches to this matter[4], and currently emerging governments' interest in regulation in this field. For instance, the mapping includes frameworks that illustrate that some governments concentrate their efforts on developing and promoting a set of voluntary technical and organizational measures, specifications, and standards, while

[4] Within the Geneva Dialogue, Nele Achten, Senior Researcher for cyber security and foreign policy at the Senior Researcher for Cybersecurity Policy at Center for Security Studies (CSS) at ETH Zurich, made the analysis of states' approaches in this regard. While the report is not yet published, it is possible to request a copy via a notification sign-up.

others focus on labelling and certification schemes for some categories of ICT products (e.g., consumer IoT or smart devices) as a way to enhance ICT supply chain security.

At the same time, varying terminology does not always entail different measures, steps and approaches. For instance, though the U.S. President's Executive Order (EO) on "Improving the Nation's Cybersecurity (14028)" issued on May 12, 2021, uses "software supply chain security" and "integrity of the software supply chain", while the 2017 Cybersecurity Act of the EU uses "ICT supply chain", they both call for transparency in product components; security during entire products' lifecycle as well as for the development of security specifications and associated conformity assessments.

Even within a single category of frameworks, readers are recommended to distinguish among different types of documents as well as consider their target audience and goals. The frameworks analyzed are not equally detailed: some outline general principles and good practices; others are very precise. Therefore, analyzing the broader context, and taking into account the aims of frameworks' initiators and the target audience without being necessarily strict on the applied terminology – these are important factors for a better understanding of their implementation and consequences.

2. Actions under the 'Responsibility and duty of care' principle are covered the most in all the types of frameworks analyzed. The 'Transparency and information sharing' principle comes second; however, the frameworks addressing this principle mostly focus on private sector entities, and not sufficiently on the public sector. The 'Innovation and competition' principle, in particular, presuming the creation of market incentives, is addressed to a lesser extent or not addressed at all in the frameworks analyzed.

All frameworks analyzed, except for some *intergovernmental frameworks* negotiated within the OSCE and UN, address the 'Responsibility and duty of care' principle, which includes practical steps, such as adopting and/or implementing security-by-design requirements, standards, certification and conformity assessments; adopting public procurement requirements; implementing dynamic management of digital security through vulnerability management, coordinated vulnerability disclosure (CVD) policies, etc. However, within this principle the existing challenge remains for addressing the EOL gap, i.e., adopting and/or implementing responsible EOL policies, and very few frameworks cover this action (A15).

As mentioned, the 'Transparency and information sharing' principle is the second most covered principle, though primarily addressing the private sector's role (what the private sector is expected and supposed to do), and not the public sector's role. This creates asymmetry in the design and delivery of measures to enhance ICT supply chain security, and puts greater responsibility on the private sector (e.g., to provide and increase transparency on processes and policies, products' code, traceability, general trustworthiness, and third-party evaluation). This is important since the private sector often owns or manages ICT systems and infrastructure. At the same time, a lack of transparency-related recommendations addressed to the public sector is evident as a result of the mapping (with the exception of the GCSC recommendations, and particularly norm 5, which calls on states to create transparent frameworks on vulnerability disclosure).

An action on creating market incentives (A22) within the 'Innovation and competition' principle is addressed to a lesser extent or not addressed at all in the frameworks analyzed. This is especially interesting in light of the broader calls from the industry's side to develop and support market incentives encouraging organizations to invest more in digital security – particularly in ICT supply chain security. This is discussed further in workstream II.

We also noticed that *public policy and standardization and labelling frameworks* rarely address an action (A5) calling to increase and provide transparency on general trustworthiness (broader ecosystem through providing a track record of the organization for managing digital security, impact of applicable domestic laws, etc.). This may indicate the governments' preference toward more technical risk-based evaluation criteria in defining ICT supply chain security, rather than toward non-technical criteria that might potentially focus on evaluating less tangible institutional environment-wide trust in an organization and/or product.

3. Some public policy frameworks welcome and encourage certifications as well as application or development of standards; however, this should be a common practice and they all should clarify what particular standards need to be implemented.

We studied some key examples among *public policy frameworks* representing relatively mature markets and, therefore, mature approaches to ICT supply chain security and digital security overall. Some frameworks e.g. the EU Cybersecurity Act and EU Toolbox on 5G cybersecurity provide information on particular standards or technical specifications. But this is not the case for all frameworks, while they are expected to provide a clearer guidance on which international standards on information security (e.g. ISO/IEC 27000-series) should be implemented. Furthermore, organizations, given their different size, operations and resources, require different security profiles, i.e. a set of baseline security requirements. Therefore, filling this knowledge gap for the public sector by providing a pro-active guidance on the amount of security obligations tailored to different organizations is the key element to the effective implementation of those obligations and overall security for all.

4. Standardization and labelling frameworks focus on instruments and tools to empower consumers and users of products.

Analyzing the selected *standardization and labelling frameworks*, we have seen the focus on recommendations and instruments to raise awareness and educate users of products (actions A7-A11 within the 'Awareness and empowerment' principle). Through promoting labels and providing "effective consumer protection" (i.e., ensuring protection of privacy, dispute resolution mechanisms, protecting consumers from hazards to their health and safety, etc.), the *standardization and labelling frameworks* make an important contribution in encouraging better security among users, and raising their awareness of 'digital hygiene' in using ICT products and services. This is an important step, in addition to promoting security-by-design industry practices, since the more security-aware and security-conscious users are, the higher users' demand for secure ICT products and services will be. And this, from an economic perspective, could potentially address the missing incentive for organizations to invest more in digital security (which we discuss in workstream II), as well as address the existing information asymmetry (when consumers and users have far less information about ICT products and services than their manufacturers).

5. **Multi-stakeholder and intergovernmental frameworks, except for the OECD report on vulnerability treatment, outline high-level and general principles without going into details on implementation, thus leaving leeway for different interpretations made by readers and recipients. Furthermore, there is a lack of intergovernmental frameworks encouraging states to adopt and implement ICT supply chain security measures.**

We have observed that *intergovernmental frameworks,* except for the OECD report on vulnerability treatment [42], tend to focus on high-level principles that leave room for interpretation, thus being considered quite flexible for recipients to implement their recommendations. This is both a positive and negative implication since, on the one hand, it could potentially attract greater support in the global community; however, their interpretation and implementation could be inconsistent at the same time.

Moreover, the mapping revealed a lack of *intergovernmental frameworks* that would encourage states to adopt and implement ICT supply chain security measures. An exception is the 2021 GGE report on cyber, which provides a thorough discussion and elaboration from states on the implementation of the norm focusing on the integrity of supply chains and responsible reporting of vulnerabilities. This report, provided by twenty-five governmental experts, is a step forward and the most detailed document providing recommendations to states for adopting certain measures.

Finally, we also note that *intergovernmental frameworks* do not address actions within the 'Transparency and information sharing' principle (A1-A6), which call for providing greater transparency on digital security, products and processes, general trustworthiness, and third-party evaluation. We understand that these are quite practical steps, which are usually aimed at the private sector – particularly ICT manufacturers. At the same time, addressing these steps and thus adding more specifications to recommendations, the *intergovernmental frameworks* could potentially attract greater interest of the private sector and thus contribute to more effective implementation. And more importantly, this could potentially help address the concerns in the global community over the fragmentation among states in approaching digital security, and ICT supply chain security in particular.

6. **The phrasing of the recommended actions in the frameworks analyzed, whether they are precise or not, rarely take into account types of recipients and their different capabilities.**

Rarely are the frameworks analyzed especially specific about different capabilities and types of their target audience; therefore, they rarely provide tailored recommendations or guidance. It may be potentially difficult, for instance, for small and medium organizations – whose role in securing ICT supply chains is equally important – to ensure their effective implementation.

7. Many of the frameworks lack coherence and synchronization among them, which makes it difficult for stakeholders to find their way in supply chain security initiatives.

During our work in 2021, we have observed continuous growth of different frameworks relating to ICT supply chain security, which, we expect, will continue beyond this year's work (and also explains why we decided to focus on key selected frameworks, giving up on the aim to cover all frameworks existing in the global community). This growth signals two positive aspects: first, where gaps exists, emerging initiatives have the potential to close them at different levels – international, regional, or local. And second, the growth of initiatives has the potential to produce a geographically diverse (as well as diverse in terms of the stakeholder groups involved) set of practical and useful steps and recommendations to enhance ICT supply chain security.

At the same time, we note the lack of coherence and synchronization among multiple frameworks, which might be challenging for stakeholders when finding their way through ICT supply chain security initiatives – especially for those who may lack resources (e.g., SMEs).

On a final note, within this chapter, we would also like to share some interesting observations that are not sure reflect bigger trends.

We did not expect to find a most overarching framework, i.e., one that could address all actions within the six OECD high-level principles. However, we were able to find frameworks (especially in public policy, standardization and labelling frameworks) that are quite detailed in terms of steps, measures and recommendations to enhance ICT supply chain security. Many of those frameworks have similarities by favoring measures to promote standards, certifications, and conformity assessments; to formulate and adopt requirements for vulnerability management and disclosure processes, as well as to increase and provide transparency on traceability (the latter is mostly formulated as a requirement to produce and provide a Software Bill of Materials (SBOM) – a concept that is gaining greater attention in industry, but still not broadly).

Taken as a whole, *corporate and non-governmental frameworks* tend to be well developed if not comprehensive, reflecting the role of the private sector in promoting good practices. However, distinctions should be made between internal policies implemented by companies, and self-regulatory codes of conduct elaborated by a group of companies, and which are recommended for implementation at their will. These frameworks also emphasize: the necessity of adopting and/or implementing security-by-design requirements, certification, standards and conformity assessments (the frameworks address each of them differently); the necessity of providing greater transparency about ICT products and services, including on third-party evaluation; the necessity of multi-stakeholder cooperation, including but not limited to security researchers, competitors, CERTs and others; and finally – the necessity of developing proportionate measures and policies through impact assessments or engaging industry's inputs. In particularly, an action (A14) focusing on the dynamic management of digital security is widely encouraged/addressed in this type of framework.

WORKSTREAM II: IMPLEMENTATION GAPS

Goal of workstream II: Identifying cases and factors leading to failure or success in implementation of the frameworks in the field of ICT supply chain security.

The mapping prepared within workstream I, as well as the public consultation launched within the Paris Call community in summer 2021, served as a basis for identifying particular incentives and factors leading to success or failure in the implementation of ICT supply chain security-related frameworks. Filling the 'implementation gap' aims to provide greater visibility of how those OECD high-level principles are already implemented in existing efforts in the global community.

The incentives identified as well as factors of success or failure can be used by policy makers and industry in exploring and developing mitigation strategies for efficient implementation of the frameworks relating to ICT supply chain security.

Key incentives

What incentivizes different stakeholder groups to care more about digital security and, particularly, implement/adopt practices for ICT supply chain security – depending on their roles (e.g., supplier, end-user, etc.)?

The key incentives can be characterized as follows:

1. Regulatory compliance and liability;
2. Market forces and economic incentives, including pressure from customers, existing and potential users, and peer pressure and competition with other actors on the global market and access to information/markets;
3. Procurement and risk mitigation needs, as well as business continuity and resilience, including the necessity to choose reliable and trustworthy ICT products and services. These incentives could be particularly relevant to organizations that are a part of ICT supply chains and which have their own need to choose reliable and trustworthy ICT products, being driven by security and/or safety factors, without government or regulatory compliance pressure;
4. Reputational incentives, including the desire to look like and be perceived as a responsible, trusted and trustworthy and, therefore, attractive actor, which could be leveraged as a market differentiator.

In the current literature (e.g. here [10]) quite often geopolitical considerations are discussed among driving factors incentivizing more security-focused thinking among organizations on the market. We do not select this as a separate bullet item, considering that geopolitical dynamics and associated restrictions on the global ICT market may be a component in all incentives mentioned above (e.g., geopolitics could impact security-focused behavior in an organization because of the need to ensure its regulatory compliance or build its own effective risk mitigation processes for business continuity and resilience).

We also discussed that the growing speed of digital transformation, accelerated by the pandemic, increases interdependency in economic sectors and in society, where organizations operate in complex, multi-dimensional and multi-directional ecosystems with, sometimes, shared risks. It forces organizations to take into account the impact of security decisions made by third-

parties in the ICT supply chains on them, including even secondary and tertiary effects on other people or businesses that might depend on what they do or do not do to prevent security and safety risks. This interdependency supported by digitalization makes all the incentives discussed above more crucial.

Depending on their region, economy or industry sector, stakeholder group, and even size (taking into account SMEs), different actors would prioritize the incentives above in a different way.

At the same time, we have identified and discussed the following incentives, which are still missing on the market and, therefore, create a gap to be further studied by stakeholder groups. These missing incentives include the following:

- **Incentives from the user side (both advanced and mainstream [5])** which could potentially incentivize, encourage or even require ICT manufacturers to invest more in security controls, and specifically to adopt or follow ICT supply chain security-related frameworks. In educating users more and raising their awareness of security and safety risks, such incentives can have a stronger impact on ICT manufacturers. However, even without a technical background, significant cybersecurity incidents might trigger both advanced and mainstream users' security-focused behavior.
- **Incentives from the government side**, which could contribute to developing economic conditions and a culture where greater security investments are encouraged and beneficial for agents to compete on the market. For instance, labelling and certifications[6], where initiated by the public sector (regulatory agencies) and which rely on existing international standards, could serve as a solution to ensure and clearly demonstrate security and safety benefits of ICT products and services, as well as help reduce information asymmetries and be used as a competitive advantage on the market. In this matter, a role of certification, that is the attestation of the robustness of a product, based on a compliance analysis and penetration tests performed by a third-party evaluator, should be particularly highlighted.
- **Incentives from government side**, which could contribute to developing an internationally interoperable and clear regulatory landscape (i.e., a set of clear policy principles and/or technical requirements and obligations that are aligned with international efforts/standards and remain interoperable across jurisdictions and sectors as much as possible). Governments' actions could also include steps to clarify the existing map of standards and how organizations can effectively navigate through it to satisfy their security needs.

[5] In the context of this report, we apply the definitions of "advanced users" and "mainstream users" following the 2021 OECD report on "Enhancing the digital security of products". "Advanced users" are those which are typically more aware and able to manage digital security risk associated with the use of ICT products and services than mainstream users. They are more experiences and autonomous users (e.g. tech savvy users in professional environments, trained security experts etc.) "Mainstream users" include consumers and some corporate users like SMEs, and they may have limited skills and knowledge about digital security, and therefore may not have the ability to accurately identify and manage digital security risk.

[6] It should be noted that labelling and certifications are not the same. Labels may or may not be regulated by a government agency, and it means any claim made on a product. A certification is a label that can only be used if the product meets certain standards set and regulated by a government agency.

- **Incentives from the private sector, and specifically from manufacturers of ICT products and services** to keep the ICT products interoperable, and to avoid creating technical and legal barriers. These barriers could be particularly challenging for security researchers to conduct vulnerability analysis in ICT products and services, leaving a large portion of them not properly tested. This could create security risks that could be further exploited by cybercriminals for conducting ICT supply chain operations. Therefore, openness to cooperation across sectors, information exchange, and responsible innovations [7]could serve as incentives for others in the market to invest more in digital security. Openness to collaboration and sharing of security best practices with others could be especially helpful for SMEs. We are also seeing that such openness can be imposed on the private sector, e.g., through anti-trust and competition regulation by governments to foster innovation).

Key factors leading to success and failure in the application and implementation of frameworks related to ICT supply chain security

Looking for views based on practical experience, we raised questions on particular success and failure stories in adopting or implementing ICT supply chain security-related frameworks. As a result, we managed to identify four groups of factors that may define further success or failure in investing more effort for stronger ICT supply chain security. The four groups include: regulatory, institutional, policy, and economic/market factors.

We detail each of them below, and explain the impacts of their implementation or lack of implementation. If the factors below are addressed or implemented, then they will most likely be considered as those leading to success in adopting ICT supply chain security practices. If the same factors remain unaddressed and not implemented, they serve as factors that would most likely lead to failure in ensuring ICT supply chain security.

[7] One of the WG6 members shared that the European Commission definition of RRI (Research and Responsible Innovation) highlights the benefits of the relation: engaging society in its research and innovation activities, increasing access to scientific results, ensuring gender equality in both the research process and research content, considering the ethical dimension, and promoting formal and informal science education. On the other hand, The European Economic and Social Committee stated that the RRI approach might harm the freedom of the mind achieved by the Enlightenment. Therefore, innovations shouldn't be seen as a risk or a threat but rather as an opportunity for progress. European Commission, Science with and for Society https://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society, accessed 1.3.2016.
Gerd Wolf, Opinion of the European Economic and Social Committee on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Research and innovation as sources of renewed growth, (COM(2014) 339 final — SWD(2014) 181 final) (2015/C 230/09), Official Journal of the European Union C 230/59, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2015.230.01.0059.01.ENG, accessed 1.3.2016.

Another member shared that responsible innovation-making includes, but is not limited to the possible misuses of technology and of data. It aims to put in place safeguards to prevent misuse and abuse. It considers the moral and ethical implications of innovation e.g. blockchain may be a strong distributed digital ledger, but should only accredited companies/organizations have access to the technology. The questions around the use, abuse, and misuse of digital tools will increase in frequency as we develop more innovations around dual-use technologies. It is important to create a culture of responsible innovation-making today. More information is available at https://www.accesspartnership.com/pathtofairtech. We welcome other views on this topic to align the understanding in the global community of what responsible innovation-making could imply.

Regulatory:

- Lack of clarity on what key security requirements, standards and regulatory obligations there are that are broadly aimed at ICT products and services within one jurisdiction or, on the contrary, the existence of numerous specifications, standards, and requirements with a lack of guidance or recommendations on their application. The lack of clarity on what the minimum security baselines are that would be deemed sufficient for ICT supply chain security create additional costs for organizations to identify them independently with a risk that they would not be sufficient overall.
- Growing fragmentation and the existence of competing or contradicting specifications/standards/requirements across multiple jurisdictions, which impose costs for organizations in both ways: in attempts (studying, hiring external consultancy) to, and failure (non-compliance fines) to ensure compliance.
- Efforts to enhance ICT supply chain security through vulnerability analysis and vulnerability disclosure, in particular, could trigger criminal or civil liability. The existing legal uncertainty or legislation that does not accept 'ethical hacking', prevents individuals or organizations to assess ICT products and thus enhance ICT supply chain resilience.

Institutional:

- Lack or absence of information on established and designated regulatory bodies that define, develop, assess and validate the compliance of policies and processes in specifications/standards/requirements.
- Lack of a clear institutional framework for organizations to follow for ICT supply chain security – creating a risk of implementation failure.

Policy[8]:

- Lack of knowledge from both markets and governments on what should be minimum security baselines for ICT supply chain security and, particularly, what should be certified and/or which risks should be mitigated.
- Lack of information as well as lack of competencies to assess what significantly-secure and insecure ICT products and services are. This is complemented by limited visibility and insight into suppliers' networks, processes and practices – both organizational and engineering (e.g., a list of code's components or SBOMs provided to customers).
- Challenges related to make certifications work and effective, including: (i) better information about which benefits the certification brings to organizations within a particular jurisdiction; (ii) in-depth certification process vs fast development of ICT products and services, as also following impulses from the market and users (a 'produce fast and fail fast' mindset); and (iii) increasing complexity of ICT products and services of a multi-component nature, which can require several certification schemes for the entire product to cover different components, and this could lead to additional costs on organizations.

[8] Policy factors differ from regulatory factors in that they speak about a lack or existence of certain policies, information and processes in a broad sense, and thus could be initiated by both the public and private sectors. The regulatory factors, in turn, strictly imply actions by regulatory agencies only to impact ICT supply chain security-related behavior on the market.

Economic/market:

- Efforts to enhance ICT supply chain security cost, and not all organizations can allow these costs (especially when there are no obvious economic or reputational reasons to bear these costs). The maturity of the market might also not be sufficient to incentivize and promote the sufficient environment and ecosystem for security-focused behavior. This could lead to rather favoring the development and sale of new products over implementing security requirements.
- Specific cross-sector limitations: e.g., legacy systems set up in two closely interdependent sub-sectors (e.g., within energy) where the update of one system would cause disruptions to the work of another and therefore impose additional costs;
- Cyberattacks and risks of being affected by them – if there is a rise of successful cyberattacks that have the potential to significantly impact business continuity, as well as cause operational disruptions and lead to financial losses, then they would serve as a factor triggering security-focused behavior and nudge greater efforts to invest in ICT supply chain security.

WORKSTREAM III: ACTIONS AREAS OF STAKEHOLDER GROUPS

Goal of workstream III: Reflecting on actionable steps and roles of different stakeholder groups to play in ensuring ICT supply chain security.

Within this workstream, we reflect on roles of different stakeholder groups to understand where they could already take actions for building stronger ICT supply chain security. The results of the two first workstreams serve as a basis for identifying key action areas, and, being guided by the six OECD high-level principles and actions, we share our suggestions on action areas that can be used by both policy makers and industry in identifying possible next actions to contribute to collective ICT supply chain security.

Action areas for different stakeholder groups in ICT supply chain security

ICT supply chain security is a collective and shared responsibility of many actors represented by different stakeholder groups. Due to the global nature of ICT supply chains, their complexity and involvement of many actors, it is not always easy to attribute particular actions to specific actors. Therefore, we take a high-level look to identify key groups of actors – or stakeholder groups as we will call them further in the text. In our work, we focus on the following stakeholder groups:

- Public sector or government, including national regulatory authorities and key decision-makers;
- Private sector, including but not limited to:
    - ICT manufacturers, who develop, produce and supply ICT products and services;
    - The cybersecurity community, including cybersecurity researchers;
    - Small and Medium Enterprises (SMEs);
    - Industry or consumer associations.
- International organizations and institutions, including standardization bodies;
- Customers and end-users, both advanced and mainstream users.

And since ensuring ICT supply chain security is a shared responsibility, there are different roles that the stakeholder groups identified above have. Due to the growing interconnectedness of processes across ICT supply chains, roles and actions by certain stakeholder groups have consequences on other actors. However, the roles and responsibility expected from stakeholder groups as well as the impact of their actions on others is not the same – some actors have more actions to take and/or are more capable of making a significant change for stronger ICT supply chain security, other actors – less. But if not all actors make their contribution to stronger ICT supply chain security, the chances of preventing security and safety risks are lower.

Matrix with action areas

Below we share our suggestions on a matrix with action areas, where each stakeholder group could contribute to building stronger ICT supply chain security. As the matrix shows, the private

sector on the supply side is among the key enablers of security practices, and has more areas to make a positive security impact on the development and use of ICT products and services.

OECD high-level principle and actions	Public sector	International organizations	Private sector on supply side (e.g. ICT manufacturers, including SMEs)	Private sector on demand side (e.g. SMEs) as well as mainstream users
Transparency and information sharing				
A1: Increasing and providing transparency on product features for digital security			✗	
A2: Increasing and providing transparency on processes and policies that are put in place by supply-side actors (e.g. end of life gap)	✗ (if it is a customer of ICT products and services)		✗	
A3: Increasing and providing transparency on the product's code	✗ (if it is a developer/producer of ICT products and services)		✗	
A4: Increasing and providing transparency on traceability (list of code components, product's value chain, data processing)	✗ (if it is both a customer and developer/product of ICT products and services)		✗	
A5: Increasing and providing transparency on general trustworthiness (broader ecosystem: track-record of the organization for managing digital security, impact of applicable domestic laws etc.)	✗ (if it is both a customer and developer/product of ICT products and services)		✗	
A6: Increasing and providing transparency on third-party evaluation (including certification, labels, security audits)	✗ (if it is both a customer and developer/product of ICT products and services)		✗	

OECD high-level principle and actions	Public sector	International organizations	Private sector on supply side (e.g. ICT manufacturers, including SMEs)	Private sector on demand side (e.g. SMEs) as well as mainstream users
Awareness and empowerment				
A7: Promoting labels	✗	✗ (and, where possible, seeking harmonization and interoperability between them across national jurisdictions)	✗, except for mainstream users (the private sector both as ICT manufacturers and customers, could initiate and participate in a voluntary industry-wide labeling scheme to help users to make better security informed decisions)	
A8: Launching awareness-raising campaigns and/or developing guidelines and/or supporting educational programs for educating mainstream users about basic digital security "hygiene"	✗, except for mainstream users (all stakeholder groups in the table have a role to play in raising awareness and educating users)			
A9: Promoting and engaging in capacity building and training programs for developing skills for SMEs	✗, except for mainstream users (all stakeholder groups in the table have a role to play in supporting SMEs, though their roles and contribution might be different depending on the context)			
A10: Providing "effective consumer protection" i.e. ensuring protection of privacy; dispute resolution mechanisms; protecting vulnerable and disadvantaged consumers; protecting consumers from hazards to their health and safety etc.	✗	✗ (and, where possible, seeking harmonization and interoperability between them across national jurisdictions)	✗	
A11: Empowering advanced users to adjust the level of digital security based on their own risk assessment (access and modify security settings; opting out from security defaults such as automatic updates etc.)	✗ (if it is a developer/producer of ICT products and services)		✗	

OECD high-level principle and actions	Public sector	International organizations	Private sector on supply side (e.g. ICT manufacturers, including SMEs)	Private sector on demand side (e.g. SMEs) as well as mainstream users
Responsibility and duty of care				
A12: Adopting and/or implementing security-by-design requirements/standards/certification/conformity assessments	✗, except for mainstream users (all stakeholder groups in the table have a role to play in developing, adopting and/or implementing security-by-design requirements, standards, certifications and conformity assessments, though their roles and contribution might be different depending on the context. International organizations and specifically standardization bodies could seek, where possible, harmonization and interoperability between such requirements, standards and certifications across national jurisdictions)			
A13: Adopting and/or implementing ex post mechanisms (e.g. insurance and liability law) and public procurement requirements	✗			
A14: Adopting and/or implementing dynamic management of digital security (vulnerability management, CVD policies, vulnerability handling processes, bug bounty programs etc.)	✗ (public sector could both develop such policies for the market and adopt them as well as a customer/end-user of ICT products and services)	✗ (international organizations could develop and seek, where possible, harmonization and interoperability between such policies across national jurisdictions)	✗ (where mainstream users could be specifically advised to follow the relevant security measures and steps for a dynamic management of digital security)	
A15: Adopting and/or implementing responsible EOL policies	✗ (public sector could both develop such policies for the market)	✗ (international organizations could develop and seek, where possible, harmonization and interoperability between such policies across national jurisdictions)	✗ (where mainstream users could be specifically advised to follow the relevant EOL policies to prevent safety and security risks)	
A16: Ensuring the digital security of organizations (e.g. adhering to international standards such as ISO 31000) and national jurisdictions	✗, except for mainstream users (all stakeholder groups in the table have a role to play in ensuring the digital security of organizations through adopting relevant security practices and following international standards. At the same time, the public sector could contribute in paritcular by developing national policies, and international organizations could help seek the harmonization/interoperability of such policies across national jurisdictions)			

OECD high-level principle and actions	Public sector	International organizations	Private sector on supply side (e.g. ICT manufacturers, including SMEs)	Private sector on demand side (e.g. SMEs) as well as mainstream users
Co-operation and governance				
A17: Increasing co-opeation amongst code owners across the value chain (through facilitating security bulletins, procurement guidelines, applying unique digital identities for processes, products and organizations)	✗	✗	✗	
A18: Promoting and engaging in multi-stakeholder cooperation which includes, but not limited to, security researchers (bug bounties, VD policies); competitors (through ISACs); CERTs; other relevant stakeholders (e.g. consumer associations)	✗, except for mainstream users (all stakeholder groups in the table have a role to play in building multi-stakeholder cooperation on ICT supply chain security, though their roles and contribution might be different depending on the context)			
A19: Adopting and/or implementing the whole-of-government approach (i.e. involving all relevant government agencies and institutions in charge of horizontal and sectoral regulations)	✗			
A20: Promoting and engaging in international co-operation	✗, except for mainstream users (all stakeholder groups in the table have a role to play in promoting and engaging in international cooperation on ICT supply chain security)			

OECD high-level principle and actions	Public sector	International organizations	Private sector on supply side (e.g. ICT manufacturers, including SMEs)	Private sector on demand side (e.g. SMEs) as well as mainstream users
Innovation and competition				
A21: Promoting and/or engaging in research and development	✗	✗ (international institutions, and specifically standardization bodies could engage in research and development projects with ICT manufacturers)	✗, except for mainstream users (private sector on both – demand and supply – sides could promote and/or engage in research and development projects for ICT supply chain security)	
A22: Creating market incentives (e.g. through simplifying regulatory compliance or creating innovative policies such as regulatory sandboxes)	✗	✗ (international institutions could help seek interoperability/harmonization in such policies across national jurisdictions)	✗ (manufacturers of ICT products and services could also incentivize other market players to invest more in ICT supply chain security)	✗ (e.g. SMEs could participate in innovative policies such as regulatory sandboxed to produce evidence-based information for developing further policies and market incentives)
A23: Encouraging and/or implementing voluntary frameworks to support competition	✗	✗ (international organizations could help seek interoperability/harmonization in such policies across national jurisdictions)	✗ (manufacturers of ICT products and services could promote openness and interoperability of their products and systems to support competition and innovation-making)	✗ (e.g. SMEs could participate in such frameworks to support competition and innovation-making)

OECD high-level principles and actions	Public sector	International organizations	Private sector on supply side (e.g. ICT manufacturers, including SMEs)	Private sector on demand side (e.g. SMEs) as well as mainstream users
Proportionality and risk management				
A24: Adopting and/or implementing risk-based multi-layered/tiered approaches	✗ (public sector could develop, adopt and implement, as a customer/end-user of ICT products and services, such approaches and policies)	✗ (international organizations could contribute to promoting such approaches and seeking their interoperability/harmonization across national jurisdictions)	✗	✗, except for mainstream users
A25: Adopting and/or developing proportionate measures and policies (through impact assessments or engaging industry's inputs)	✗	✗ (with regard to developing and promoting international standards or policies)	✗ (with regard to certain policies or new rules for the use of their ICT products and services)	

Some examples of concrete actions for each stakeholders groups

As provided in the tables above, all stakeholder groups have a role to play in different areas, given their resources, to ensure ICT supply chain security. Below we summarize and give some examples of concrete actions that stakeholders groups in the table above could take and thus contribute to stronger security across global ICT supply chains:

International institutions (including standardization bodies)

- Developing ICT supply chain risk management policies (e.g., actions A12, A14 and 15 on security-by-design, dynamic management of digital security and responsible end-of-life policies);
- Providing coherence and synchronization among multiple frameworks to reduce fragmentation across sectors and national jurisdictions as well as provide a platform for states to cooperate and develop interoperable ICT supply chain risk management policies, standards, certifications, conformity assessments and labelling schemes;
- Encouraging further both the public and private sector to enhance transparency and information sharing (i.e., actions A1-A6) and, particularly, promoting transparency in vulnerability discovery and treatment, including through increasing cooperation among code owners across the value chain (i.e., A17) and promoting multi-stakeholder cooperation on vulnerability discovery and disclosure (i.e., A18);

- Seeking complementarity and communication among the various processes on digital security, including ICT supply chain security by international institutions and standardization bodies.

Public sector (including national governments and regulatory agencies)

- Developing a national harmonized institutional framework, based on the whole-of-the government approach, on digital security and ICT supply chain security, including designating relevant competent authorities, providing guidance on what particular sector-specific standards and security measures should be implemented and would be considered sufficient for optimal security. Practically, manufacturers and customers of ICT products and services need to know what the optimal level of security is and how, in an ongoing effort, it can be achieved. This should be approached while keeping in mind the existing complexity of regulatory approaches across national jurisdictions as well as complexity of modern ICT products and services.
- Engaging in a broader dialogue with the private sector, technical experts and other states to develop and provide interoperable sector-specific security baselines as well as to identify the need for certification, conformity assessments and labeling schemes for particular types of ICT products and services and with several layers of risk attestation (from baseline to the most advanced);
- Adopting a risk-based multi-layered approach to developing standards and/or security baselines and/or labelling schemes for particular types of ICT products and services to identify several layers of security assurance and thus provide flexibility for manufacturers, given their varying resources and capacities to compete as well as given the various criticality of ICT products and services they produce;
- Developing a security-focused culture across different sectors and stakeholder groups, including mainstream users, through continuous and ongoing educating and raising awareness to make sure they are sufficiently informed about their duty of care in using ICTs;
- Creating the right economic environment to incentivize manufacturers and consumers, including SMEs in both cases, which often lack resources and capacities, with certain targeted policy tools that would be part of the common technology ecosystem. In building closer dialogues and trusted partnerships with companies of any size, the public sector's role is to shape the rules so that cybersecurity becomes a competitive advantage;
- Adopting the 'carrot rather than stick' approach where the private sector – both on the supply and demand sides – is incentivized to adopt ICT supply chain security measures for clear and tangible benefits. Programs offering cashbacks and financial bonuses for cyber insurance to companies adopting stronger security controls could be an option to explore further for specific sectors and types of ICT products and services. Projects exploring cyber ratings in assessing security-advanced ICT products and services could serve as an incentive for manufacturers to compete in this field as well;

- Stimulating educational programs and research and development investments through closer capacity building partnerships with companies of any size, where needed, to address the lack of resources, capacities and knowledge on security practices among market players, including SMEs;
- Incentivizing responsible vulnerability treatment on both the demand and supply sides through developing guidance and recommendations to establish relevant processes for dynamic management of digital security;
- Updating the national legal framework, where possible, to incentivize ethical cybersecurity research and vulnerability analysis for assessing modern ICT products and services against exploitable vulnerabilities and, therefore, significant security risks to users;
- Promoting transparency on vulnerability treatment through the Vulnerability Equities Process (VEP);
- Developing a robust and functioning market for insurance products through claims-adjuster training and certification; underwriter training and certification; developing frameworks and research methodologies for understanding and accurately pricing cyber risks; identifying common areas of interest for donating and pooling anonymized data that can be used for more accurate risk models;
- Developing policy actions tackling the end-of-life (EOL) gap through, e.g., requiring supply-side actors to design and implement clear and transparent EOL policies for their ICT products and services, and publicly stating the minimum length of time for which a product would be provided with security updates;
- Implementing non-binding norms on supply chain integrity and responsible reporting of vulnerabilities, as adopted by the Group of Governmental Experts and further elaborated in 2021 [7].

Private sector on supply side (including SMEs)

- Adopting and implementing security-by-design requirements and embedding security into software development of ICT products and services; adopting and implementing security baseline requirements, including on product security and data protection;
- Adopting and continuously implementing dynamic management of digital security (such as vulnerability disclosure and, broadly, vulnerability treatment policies);
- Adopting and implementing clear, transparent and sustainable EOL policies to provide sufficient information to end-users about the stage of the ICT products' lifecycle when security updates would be no longer available;
- Implementing third-party security assessments, certifications and participating in labeling schemes, where possible, to provide greater security assurance to customers and end-users;
- Producing and providing greater transparency about ICT products and services (i.e., actions A1-A6) as well as providing guidance and recommendations – in user-friendly and plain language – on functionality, use cases, safety and security of ICT products and services;

- Implementing and maintaining a bill of materials, where possible taking into account sector specificity, criticality and capacities available, to have an inventory of software components, information about those components, and the relationships between them for more effective vulnerability management, disclosure and overall ICT supply chain risk management;
- Engaging ethical cybersecurity researchers to assess ICT products and services against exploitable vulnerabilities and significant risks to users. Bug bounty programs could be considered as an option to provide greater transparency on the scope, liability rules and communication protocol for accepting vulnerability reports;
- Engaging in existing public-private, or non-governmental, or multistakeholder and other frameworks and partnerships to team up with public and private sector actors to adopt and promote ICT supply chain security practices, exchange information and share best practices;
- Engaging in cyber capacity building efforts to support actors with less capacities and resources to protect against ICT supply chain risks as well as participating in awareness-raising programs and campaigns to educate end-users on digital security;
- Supporting states in the implementation of the UN GGE norms on integrity of supply chains and responsible reporting of vulnerabilities.

Private sector on demand side (including SMEs)

- Engaging in existing public-private, or non-governmental, or multistakeholder and other frameworks and partnerships to team up with public and private sector actors to adopt and promote ICT supply chain security practices;
- Adopting a security-focused approach to ICT procurement processes and maintenance of ICT products and services to prevent cybersecurity incidents and data breaches. For this, the following could be advised:
    - Optimizing financial and human resources to adopt the existing industry best practices and baselines on ICT supply chain security;
    - Adopting a risk-based approach in assessing ICT products and services and third-party suppliers;
    - Requesting a bill of materials, where possible taking into account sector specificity, criticality and capacities available, to have an inventory of software components, information about those components, and the relationships between them for more effective vulnerability management, disclosure and overall ICT supply chain risk management.

Mainstream users

- Learning about the security and functionality of ICT products and services to use them in accordance with the intended use developed by manufacturers;
- Learning about user rights and seeking customer support and protection from ICT manufacturers if there is an issue with the functionality of ICT products or services;
- Installing patches and updating ICT products and services on time to avoid security and safety risks;
- Consulting with the EOL policies or requesting them from the ICT manufacturer to replace or stop using an ICT product once it reaches the EOL, and recycle materials contained in ICT equipment, where possible, to avoid security and safety risks.

CONCLUSIONS AND RECOMMENDATIONS

1. **All actors have a role to play in building stronger ICT supply chain security. And if some actors do not make their contribution, there are higher security and safety risks for all across supply chains. To identify for actors their possible contribution, we have prepared a matrix with suggestions on pragmatic, practical actions to make a positive security impact.**

ICT supply chain security is a shared responsibility and action. Success in achieving our common security across global ICT supply chains is a sum of collective steps taken by different stakeholder groups, including the public and private sector, advanced and mainstream users, and others. Customer and end-user awareness also plays an important role in ensuring security and avoiding both security and safety risks.

2. **Build on what already exist: there are already many existing ICT supply chain security frameworks where actors can participate or use their outcomes for making both individual and collective impacts for stronger ICT supply chain security.**

The mapping we have prepared (provided in the addendum) can serve as a useful guide for the Paris Call community and beyond to identify where their organizations could participate to mature their own processes and knowledge of ICT supply chain security, exchange information with other actors and explore opportunities for mutually beneficial partnerships. Some of the frameworks (public policy, standardization and labelling, corporate and non-governmental, as well as public-private and intergovernmental) studied already provide useful guidance on certain areas to improve ICT supply chain security.

3. **However, certain areas require further action: ensuring harmonization across emerging national regulatory and industry approaches; creating incentives for security-focused behavior on both supply and demand side; and further enhancing ICT supply chain transparency by both the public and private sector.**

Our mapping identified particular areas which are least addressed by the existing ICT supply chain security frameworks we studied. For instance, the EOL gap has been addressed to a lesser extent and therefore requires further discussion by policy makers and industry to prevent security and safety risks for users. In addition, few frameworks on ICT supply chain security address the creation of market incentives or transparency-related recommendations or practical ICT supply chain security measures for the public sector. Stimulating security-focused behavior on both the supply and demand side could be an area for further action to create targeted and specific incentives. Examples of possible incentives could include, but are not limited to:

- For the supply side: introduction of cyber risk assessment models and ratings for ICT products and services; adoption of independent third-party evaluation and security attestation; and linking cyber insurance payouts; and programs with continuous security efforts;
- For the demand side: providing user-friendly transparent instruction on the use and application of ICT products and services; educating both advanced and mainstream users on security aspects; and providing effective consumer protection.

4. Ensuring the security of ICT products and services is a continuous effort, throughout the deployment lifecycle, to protect customers and end-users, that's why certifications, conformity assessments and labels should not be an end state.

As the matrix shows, the private sector on the supply side is among the key enablers of security practices and has more areas to make a positive security impact on the development and use of ICT products and services. However, there are incentives still missing, and as such are not being implemented to have greater security in modern ICT product and services. We identified several of them as well as four groups of factors leading to success or failure in the adoption of security practices, and, in particular, hope that policy makers would take a greater role in producing risk-based interoperable regulatory approaches for the ICT industry.

5. Interoperability, harmonization [9] and reciprocity on international and national levels are key in making emerging national regulatory approaches work and produce a positive economic and security impact.

Given the global nature of ICT supply chains, i.e., the fact that ICT products and services are developed, distributed, supplied, maintained and used across the globe and national jurisdictions, it is important to avoid fragmentation in emerging regulation approaches, otherwise a set of complex regulatory pieces and security requirements would create negative economic and security effects.

6. In this regard, we call for strengthening cooperation across all levels and sectors

– between digital security experts and ICT manufacturers to implement security-by-design practices; between the private sector and public sector to broadly develop risk-based effective regulatory approaches; and between states and international organizations to ensure interoperability and harmonization in current and future regulation of ICT supply chain security efforts.

[9] How is interoperability different from harmonization? We view interoperability as a characteristic of existing, emerging or future regulatory and industry approaches to 'work' with other and be complementary. Harmonization to us means the process of making those approaches similar, and where possible are the same.

ANNEX: ICT supply chain-related frameworks analyzed

The following frameworks have been identified through the consultation with WG6 members, and subsequently analyzed in the mapping:

Public policy frameworks:

- EU Cybersecurity Act [11];
- EU Toolbox on 5G Cybersecurity [12];
- EU ENISA Guidelines on Security IoT Supply Chain (2020) [13];
- EU NIS Directive (2016) [14];
- ENISA's Indispensable Baseline Security Requirements (2017) [15];
- UK Code of Practice for Consumer IoT Security [16];
- MITRE ATT&CK® [17];
- U.S. NIST 'Supply Chain Risk Management Practices for Federal Information Systems and Organizations' (Draft NIST SP 800-161, Revision 1, April 2021) [18];
- U.S. NIST White paper on 'Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)' April 2020 [19];
- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [20];
- Executive Order on Improving the Nation's Cybersecurity, May 2021 [21];
- National Security Directive on Telecom Sector, India, 2020 [22];
- Cyber Supply Chain Risk Management Practitioners Guide, Australian Cyber Security Centre (ACSC) (June 2019) [23];

Standardization & labelling frameworks:

- ETSI Standard on IoT / ETSI EN 303 645 V2.1.1 [24];
- ECSO's Label Cybersecurity Made In Europe [25];
- Singapore Cybersecurity Labelling Scheme (CLS) [26];
- Cyber Essentials UK[27]; Cyber Secure Canada [28];
- Cybersecurity Maturity Model Certification (CMMC) [29];

Corporate & non-governmental frameworks:

- Cybersecurity Tech Accord [30];
- Kaspersky Global Transparency Initiative [31];
- Charter of Trust [32];
- EastWest Institute (EWI)'s Buyers Guide ('Purchasing Secure ICT Products and Services') [33];

- EWI's Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk ('Weathering TechNationalism') [34];
- Carnegie Paper on "ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies" (October 2019) [35];

Public-private collaborative frameworks:

- Paris Call for Trust and Security in Cyberspace [36];
- Geneva Dialogue on responsible behavior in cyberspace (including the 2020 Output document on 'Security of digital products and services: Reducing vulnerabilities and secure design: Good practices') [37];
- Global Commission on the Stability of Cyberspace: 2019 Final report [38];

Intergovernmental frameworks:

- UN GGE 2015 report [39]; UN GGE 2021 report [40];
- OSCE Decision n°1202, 10 March 2016 [41];
- OECD report on 'Encouraging vulnerability treatment: responsible management, handling and disclosure of vulnerabilities' (2021) [42];
- A/RES/57/239 «Creation of a global culture of cybersecurity» (31 January 2003) [43];
- A/RES/73/27 on "Developments in the field of information and telecommunications in the context of international security" (11 December 2018) [44];
- A/75/816 Final Substantive Report of the UN OEWG on developments in the field of information and telecommunications in the context of international security [45].

REFERENCES

1. Report of the UN GGE 2015 A/70/174, https://undocs.org/A/70/174; Report of the UN GGE 2021 A/76/135; https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf; UN GA Resolution A/RES/73/27, https://undocs.org/en/A/RES/73/27; Report of the UN OEWG 2021 A/75/8162 https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
2. Paris Call, https://pariscall.international/en/
3. Paris Call's principles : https://pariscall.international/en/principles
4. Speech at the PPF 2020 : A path towards trust and security in the Cyberspace: building further upon the Paris Call https://www.youtube.com/watch?v=zaCgxD0FFRI:Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 28 May 2021 https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf
5. Enhancing the digital security of products: A policy discussion, OECD Digital Economy Papers, No. 306, OECD Publishing, Paris https://doi.org/10.1787/cd9f9ebc-en
6. OECD 2021 report on the Digital Security of Products https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-digital-security-of-products_cd9f9ebc-en
7. Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk : https://www.eastwest.ngo/sites/default/files/ideas-files/weathering-technationalism.pdf
8. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), Eur-Lex, https://eur-lex.europa.eu/eli/reg/2019/881/oj
9. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, European Commission, 29 January 2020 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
10. IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain, European Union Agency for Cybersecurity, 9 Novembre 2020 https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain
11. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016, p. 1–30, Eur-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148
12. Indispensable baseline security requirements for the procurement of secure ICT products and services, European Union Agency for Cybersecurity, 21 January 2017, https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services

13. Code of Practice for Consumer IoT Security, Department for Digital, Culture, Media & Sport, Gov.uk, 14 October 2018 https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

14. ATT&CK Matrix for Enterprise, MITRE ATT&CK®, https://attack.mitre.org

15. Cyber Supply Chain Risk Management Practices for Systems and Organizations, aft NIST Special Publication 800-161 Revision 1, April 2021 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft.pdf

16. Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), Nist Cybersecurity White Paper, 23 April 2020 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf

17. REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, Official Journal of the European Union, 5 April 2017 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

18. Executive Order on Improving the Nation's Cybersecurity, The White House, 12 May 2021 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

19. National security directive in telecoms sector to boost use of homegrown gear: TEMA, ET Telecom, 18 December 2020 https://telecom.economictimes.indiatimes.com/news/national-security-directive-in-telecoms-sector-to-boost-use-of-homegrown-gear-tema/79794418

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

21. Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI, 2020 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

22. Cybersecurity Made in Europe - For a stronger and more competitive European cybersecurity market, European Cyber Security Organisation, https://ecs-org.eu/working-groups/cybersecurity-made-in-europe

23. Cybersecurity Labelling Scheme (CLS), CSA Singapore, https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls

24. Cyber essentials, National Cyber Security Centre, https://www.ncsc.gov.uk/cyberessentials/overview

25. Cyber Secure Canada, https://www.ic.gc.ca/eic/site/137.nsf/eng/home

26. Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification, https://www.acq.osd.mil/cmmc/

27. Cybersecurity Tech Accord, https://cybertechaccord.org

28. Kaspersky Global Transparency Initiative, https://www.kaspersky.com/transparency-center

29. Kaspersky Transparency Center, https://www.kaspersky.com/transparency-center-offices

30. Kaspersky Cyber Capacity Building , https://www.kaspersky.com/capacity-building

31. Charter of Trust, https://www.charteroftrust.com

32. Purchasing Secure ICT Products and Services: A Buyers Guide, East West Institute, https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf

33. Weathering TechNationalism, Policy Report, Alex W. Schulman, 18 May 2020

34. ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies, Ariel (Eli) Levite, Carnegie Endowment For International Peace, 4 October 2019, https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974

35. Carnegie Paper on "ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies", October 2019, https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974

36. Geneva Dialogue On Responsible Behaviour in Cyberespace, https://genevadialogue.ch

37. Security of digital products and services: Reducing vulnerabilities and secure design - Industry Good Practices, Geneva Dialogue On Responsible Behaviour in Cyberespace, December 2020, https://genevadialogue.ch/goodpractices/

38. Advancing Cyberstability Final Report, November 2019, Global Commission on the Stability of Cyberespace, https://cyberstability.org/report/

39. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations, 22 July 2015, https://documents-dds ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

40. Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 28 May 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

41. OSCE Confidence-Building measures to reduce the risks of conflict stemming from the use of information and communication technologies, Organization for Security and Co-operation in Europe Permanent Council, 10 March 2016, https://www.osce.org/files/f/documents/d/a/227281.pdf

42. Encouraging vulnerability treatment - How policy makers can help address digital security vulnerabilities, STI Policy Note (OECD), February 2021, https://www.oecd.org/digital/encouraging-vulnerability-treatment.pdf

43. Creation of a global culture of cybersecurity : resolution / adopted by the General Assembly, UN. General Assembly, 2003, https://digitallibrary.un.org/record/482184?ln=en

44. Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly, UN General Assembly, 2018, https://digitallibrary.un.org/record/1655670?ln=en

45. Open-ended working group on developments in the field of information and telecommunications in the context of international security, United Nations General Assembly, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

About the Paris Call

The Paris Call for Trust and Security in Cyberspace, launched by President Macron in November 2018, promotes a multi-stakeholder approach to the regulation of cyberspace in collaboration with States, private sector entities and civil society organizations. The Paris Call is now the largest international, multi-stakeholder initiative on cybersecurity with 1 100 supporters from all regions of the world.
Learn more at https://pariscall.international/en/.

About Cigref

Created in 1970, Cigref is a non-profit organisation representing the largest French companies and public administrations, exclusively users of digital solutions and services, which supports its members in their collective thinking on digital issues. Cigref's 152 members represent 1700 billion in cumulative sales, 9 million employees supplied internally with IT solutions and services by more than 200,000 professionals. Our association works, for the benefit of its members, in favour of a sustainable, responsible and trustworthy digital environment.
Learn more at www.cigref.fr.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 250,000 corporate clients protect what matters most to them. Kaspersky has been one of the early signatories of the Paris Call for Trust and Security in Cyberspace and supported the second edition of the global Paris Peace Forum in 2019.
Learn more at www.kaspersky.com

About GEODE

GEODE (Geopolitics of the Datasphere) is a research and training center at the University of Paris 8 dedicated to the study of the impact of digital transformation on the strategic environment. It has been selected for a "Center of Excellence for International Relations and Strategy" label by the French Ministry of the Army. Its scientific ambition is twofold. On the one hand, to use the resources of the datasphere for geopolitical analysis, i.e. to develop tools to collect, process, and exploit the large masses of data relating to the datasphere, and to propose the development of new methods for mapping physical spaces based on the fusion of spatialized and non-spatialized data. And on the other hand, to study the datasphere as a geopolitical object in its own right.
Learn more at https://geode.science/en/home-2/