GENEVA DIALOGUE
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

Governance Approaches to the Security of Digital Products

A COMPARATIVE ANALYSIS

November 24, 2021

CSS
ETH Zürich

Acknowledgments

This report was commissioned by the Swiss Federal Department of Foreign Affairs (FDFA) in order to support the Geneva Dialogue of Responsible Behavior in Cyberspace. The scope of the report was continuously discussed with Jonas Grätz-Hoffmann (FDFA) and Vladimir Radunovic (Diplo Foundation). The author would like to thank both for an excellent cooperation and their willingness to share contacts and information within and from their respective networks. The report also benefitted from inputs from the Swiss embassies in Austria, China, Germany, Singapore and India, who helped to gather background information in the respective countries.

To elaborate on the digital product security challenges policymaker are facing, the author of the report conducted interviews with public officials from the following public agencies:

- Australia's Department of Home Affairs
- European Commission, Directorate General for Communications Networks, Content and Technology
- German Federal Office for Information Security
- German Federal Ministry of the Interior, Building and Community
- Israeli National Cyber Directorate
- United Kingdom Department for Digital, Culture, Media & Sport
- United States Department of Commerce, National Institute of Standards and Technology & National Telecommunications and Information Administration
- Cyber Security Agency of Singapore

The author would like to thank the interview partners for their time and candid insights into their domestic policies, laws and planned future activities in this space. Without their willingness to share their expertise and the challenges they face, it would not have been possible to write this report. In addition, the author is grateful for the support of numerous individuals in industry, civil society and academia who helped to identify relevant interview partners in the selected jurisdictions.

The report was proofread and edited by my colleagues at the Center for Security Studies at ETH Zürich. I would like to thank in particular my colleague Jakob Bund, who was always available for discussions and feedback; Sean Cordey for the final review and Allison Chandley for proofreading.

Author: Nele Achten, Senior researcher for cybersecurity policy, Center for Security Studies, ETH Zürich

Contents

Key Insights

1. **Security of digital products** is a relatively **new regulatory field** that can be placed somewhere **between data security regulations and critical infrastructure protection** (CIP). While there is a significant overlap between product security and security of critical infrastructure (CI) (e.g., cloud services can be both), the type of rules governing both regulatory fields are generally different. Most policies and mandatory rules for CI providers have focused on best practices to strengthen the security of the organization. By contrast, emerging policies and legal frameworks addressing the security of digital products focus on security measures during the development and lifecycle of the product.

2. **Digital products** can be all types of **software, hardware or a combination thereof**. Public agencies mostly address software, Internet of Things (IoT) devices and sometimes cloud services in their policies of digital products. Industry tends to have a broader understanding of digital products, including 5G and AI technologies. Policy documents and public commitments to strengthen security use the term digital products. **Legal documents and guidelines establishing security objectives or proposing concrete measures**, however, **mostly distinguish between different types of technologies**. The question arises whether it is possible to develop horizontal security requirements for all types of digital products or whether a distinction is required in order to effectively improve security of digital products.

3. The depth of security regulations in the digital space differs among jurisdictions. Some jurisdictions also use different legal concepts for different policy tools. One policy tool discussed in a number of jurisdictions is the adoption of **mandatory minimum baseline requirements**. Maybe unexpectedly, industry representatives have signaled support for such an approach. One reason for their support might be that these minimum baseline requirements are mostly **prescriptive, easy to implement** and often consist of **low security standards**. These low standards often prove less stringent than the existing practices of big companies engaged in these policy discussions.

4. Currently, most **security standards** developed with the **goal of being applied in a broad number of jurisdictions**. Even if they are developed by national, regional and international organizations at the same time, there are efforts to build upon each other. While a number of **bilateral agreements recognize certificates** from another country, discussions about **labels usually focus on their domestic application only**.

Acronyms

AI: Artificial Intelligence

CI: Critical Infrastructure

CIP: Critical Infrastructure Protection

ENISA: European Union Agency for Cybersecurity

ETSI: European Telecommunications Standards Institute

Geneva Dialogue: Geneva Dialogue on Responsible Behavior in Cyberspace

FDFA: Swiss Federal Department of Foreign Affairs

ICTs: Information and Communication Technologies

IoT: Internet of Things

ISO: International Organization for Standardization

NIS Directive: Network and Information Security Directive

NIST: United States National Institute for Standards and Technology

NTIA: United States National Telecommunications and Information Administration

OECD: Organization for Economic Co-operation and Development

UNGGE: United Nations Group of Governmental Experts

1 Introduction

The objective of this report is to provide an overview of regulatory frameworks that aim to strengthen the security of digital products. It is primarily for public officials working in Foreign Ministries, public policy managers in industry and other stakeholders involved in global policy processes. The Geneva Dialogue on Responsible Behavior in Cyberspace (Geneva Dialogue), a dialogue platform of experts from industry and private sector associations working on improving cybersecurity, identified regulation as a key factor to be addressed in its 2021 program. This report was first presented to approximately 70 participants from industry, civil society, governmental agencies and ministries at a Geneva Dialogue event dedicated to the security of digital products and their regulatory environment in September 2021.

The security of digital products is a policy field that has been the subject of significant interest over the past couple of years. The field is relevant for international policy dialogues because it is concerned with systemic vulnerabilities and cross-border threats to national economies and societies. In this regard, digital product security is similar to more established policies of critical infrastructure protection (CIP). However, governance approaches to the security of digital products are different from CIP in two main aspects: First, the security of digital products is focused on the vulnerabilities of the products themselves, at every stage of their life cycle. In contrast, CIP addresses security practices in the *organizations* providing the service. Second, the same product can be sold in a number of jurisdictions and the lack of policy harmonization can lead to more negative economic impact than is the case with regard to CIP.[1]

1.1 Background of the Geneva Dialogue

The Geneva Dialogue was initiated in 2018 after the failure of the UN Group of Governmental Experts (UNGGE) 2016/2017. After the failure of the UNGGE, many stakeholders highlighted the urgency to continue discussions about responsible behavior in cyberspace and the need to include the private sector into these debates. The private sector itself came up with a number of initiatives and guidelines. For example, the Charter of Trust (02/2018), the Cybersecurity Tech Accord (04/2018), the Paris Call for Trust and Security in Cyberspace (12/2018), and the Global Commission on the Stability of Cyberspace (final report 11/2019) all created new norms and expectations on strengthening cybersecurity globally and what responsible behavior in cyberspace should look like. At this time, the Swiss government created the Geneva Dialogue in order to engage in a dialogue with industry and to discuss the responsibilities of the private sector in strengthening cybersecurity.

While the responsibility of states in securing cyberspace has been the main topic of international law and norm debates for a long time, the responsibilities of the private sector in preventing large-scale cyber incidents and strengthening security gained greater prominence starting in 2018. The objective of the Geneva Dialogue was to build on this movement and to include industry, civil society and academia into international norm debates on cybersecurity. In its first phase, the Geneva Dialogue analyzed the roles and responsibilities of states, industry, civil society and academia in contributing to greater security and stability in cyberspace.[2]

Since 2020, the Geneva Dialogue has been in its second phase of operations, serving as a platform to discuss best practices, challenges and concerns regarding the security of digital products between state and

[1] Operations of CI providers are traditionally limited to a particular territory (e.g. healthcare sector providers). This assessment may change if entities such as cloud providers are defined as critical infrastructure.
[2] Website of the Geneva Dialogue on Responsible Behavior in Cyberspace 'Phase 1'.

industry representatives. The objective of the ongoing discussions is to "shape a joint vision regarding the security of digital products with leading businesses."[3] Representatives from industry, civil society and academia have met on a bi-weekly basis over the course of the last two years (Track 1 part of the Geneva Dialogue). These discussions are complemented by three half-day conferences (Track 2 part of the Geneva Dialogue) focusing on "standardization" (May 2021), "regulation" (September 2021) and "global norms" (tentatively planned for early 2022). The track 2 conferences included a broader audience, including representatives from standardization organizations and regulatory agencies.

The security of digital products has also been part of discussions in other fora. The OECD, for example, is currently negotiating a new recommendation on the digital security of products. These efforts also include the publication of an in-depth analysis, a policy discussion and a policy brief on the "digital security of products".[4]

1.2 Structure of the report

This report is based on an analysis of public policies, guides of practice, laws and administrative acts from various jurisdictions (see Annex 2). In order to better understand the practical meaning of these documents and initiatives, interviews were conducted with public officials from Australia, the European Commission, Germany, Israel, United Kingdom, United States of America and Singapore. Unfortunately, attempts to identify and talk to public officials from Russia and China were not successful.

Chapter 2 explores public guidelines and regulations aiming to strengthen the security of digital products. Based on the interviews conducted for this report, the chapter summarizes the challenges that policymakers commonly face when mandated to strengthen the security of products through guidelines or rules. It concludes with a discussion of the meaning and use of the term 'digital products' across both international and domestic policy documents and legislation.

The report addresses two legal aspects of regulating digital product security in more detail in chapter 3. First, it outlines how the attempt to regulate digital products differs from previous public cybersecurity policies and constitutes a relatively new regulatory field compared to data security and CIP regulations. Second, the report provides an overview of common legal concepts that regulators and public policymakers may choose to use in different policy tools. Notably, this report focus on public policies and regulations. It does not cover industry policies or international standards. International standards are only mentioned in situations where they serve as the basis of domestic regulations and legislation.

With the Geneva Dialogue's objective to address global policy challenges in mind, chapter 4 focuses on the risk of fragmentation emerging from different domestic regulations. This section elaborates the meaning of standards, certification and labels and the different degree of international cooperation within each of these policy areas. In addition, the chapter enlists some of the recently created fora mentioned during the interviews.

Finally, the concluding chapter suggests areas where public guidelines and regulation will likely emerge in the upcoming years. It highlights unresolved questions that should be addressed in order to advance in international policy discussions.[5]

[3] Website of the Geneva Dialogue on Responsible Behavior in Cyberspace.
[4] See OECD analysis 'Understanding the digital security of products: an in-depth analysis' (2021).
[5] See chapter 5.

Given this report's intention to provide an overview of public guidance and regulations concerning digital products, a specific example of governance approaches related to one particular digital product would have been outside the reports scope. However, many interview partners immediately understood 'security of consumer IoT devices' when they were asked about the 'digital product security' policies. Public guidance and regulations regarding consumer IoT devices are indeed more mature than the security governance of other digital products, including cloud services, 5G and AI systems. Considering that the insights to public policies on consumer IoT devices might potentially be of interest for public policymakers form jurisdictions less advanced on this topic, they are shared in Annex 1.

2 Public instruments aiming to strengthen the security of digital products

The regulation of security aspects of products and services is often interlinked with the development and use of guidelines published by state agencies. In the context of digital products, many states have produced voluntary guidelines addressing the security of consumer IoT devices[6], cloud services[7] and 5G technologies.[8] Typically, voluntary guidelines are the result of a dialogue between stakeholders from the public and private sectors. In many ways, the process of developing voluntary guidelines is comparable to developing technical and organizational standards. In some cases, voluntary guidelines were indeed accompanied by the development of an international standard. The ETSI standards 303 645 on "Cyber Security for Consumer Internet of Things", for example, were developed on the basis of the UK Code of Practice for Consumer IoT devices.[9]

This section first outlines the common challenges identified by public officials developing public policies and regulations aiming to strengthen the security of digital products. Second, it explores the use and meaning of the term 'digital products.' While this term is widely used in international and some national policy documents, it is seen less often in practical guidelines or regulations establishing concrete responsibilities of stakeholders.

2.1 Common challenges in developing public policies and regulations

For this report, the author asked public officials working on security standards and regulations what they consider to be the main challenges to their work. Some of their answers might seem familiar to those working in the field of product safety, its standardization and domestic regulation. There are however some aspects that are different, particularly in relation to domestic implementation of security standards.

[6] ENISA 'Baseline security IoT' (2017); UK Department for Digital, Culture, Media & Sport 'Code of Practice for Consumer IoT Security' (2018); NIST 'Defining IoT Cybersecurity Requirements: Draft Guidance for Federal Agencies and IoT Device Manufacturers (SP 800-213, NISTIRs 8259B/C/D)' (2020).
[7] ENISA 'EUCS Cloud Service Scheme – EUCS, a candidate cybersecurity certification scheme for cloud services' (2020).
[8] EU NIS Cooperation Group 'Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures' (2020).
[9] ETSI 303 645 v.2.1.0 'Cyber Security for Consumer Internet of Things – Baseline Requirements: Introduction' (2020); UK Department for Digital, Culture, Media and Sport 'Code of Practice for Consumer IoT security' (2018).

2.1.1 Challenge 1: Market disruption

Most interview partners were concerned about the impact that mandatory security requirements for digital products might have on the global economy. In order to mitigate the potential negative consequences, both the harmonization of standards as well as the mutual recognition of standards were identified as crucial elements of regulating the security of digital products. Another approach that may help to mitigate any disruptive effects is the prioritization of voluntary schemes over mandatory ones.[10]

Within the European Union, the potential disruptive effect of mandatory security requirements has practical consequences. Mandatory requirements adopted by one single EU member state alone would likely violate the fundamental freedoms of the EU internal market. In order to avoid a disruption of the EU internal market, any mandatory requirements will thus likely have to come from the European level.

2.1.2 Challenge 2: Making software and product developers care

A challenge that arises from voluntary requirements is how to make industry and product developers care about implementation. In the early years of the Internet, security was often not an issue that software and product developers considered. There was less awareness of potential threats and bringing innovative products to the market as quickly as possible was the key to success. Due to major cyber incidents and evolving legal requirements, most companies now consider security risks related to their products in the earliest stages of product design.

However, the public cannot assess whether a company has sufficiently prioritized security in its operations. Did the software or product developers consider potential cyber risks during the design phase and until the determined end-of-support of their product or service? The moment a major cyber incident occurs, the public certainly is justified in doubting whether a company has done enough to avoid foreseeable harm.

One major challenge for a regulatory approach is the supervision and control of implementation. It remains to be seen whether legal provisions alone are able to foster security cultures within private companies that result in adequate protection of the products and services they are offering. There is broad agreement that a mere obligation of companies and developers to ‚tick a box' do not lead to the adoption of the best possible security measures.[11] It is however easier for state agencies and independent testing or certification offices to supervise the implementation of basic security requirements that can be simplified to that degree.

Some interview partners have thought about other approaches to strengthen security practices for digital products. One interview partner pointed out that his agency has critically reflected whether legal requirements are effective to establish better security practices while considering other ways the state could support good security practices. The interview partner highlighted the challenge of his agency to accurately measure whether a particular legal requirement would led to more security.

[10] Note that a voluntary approach was already developed in the context of security practices of critical infrastructure providers and other organizations (see e.g. NIST Framework for Improving Critical Infrastructure Cybersecurity). In the context of digital products, which are manufactured in one country, sold in another country and eventually used in a third country, the risk of market disruption is much greater.

[11] Note that compliance-based security might lead to better security practices in the context of less mature products and smaller companies. However, bigger companies are often already going beyond the security requirements required by law.

Does a mandatory security officer within every company lead towards more security? What are the costs and benefits of certain specific legal requirements?

Another interview partner pointed out that the involvement of technical experts in the development of adequate standards is crucial. Engineers care more about a standard if the standard also brings a practical benefit to their work.

2.1.3 Challenge 3: Adapting to changing threat landscapes

Finally, some interview partners identified the rapid change of the threat landscape as a major challenge for their work. The prioritization of one group of threats (e.g. supply chain threats or ransomware threats) over another can change radically from one year to another. After major cyber incidents, policy and legal debates often focus on the particular vulnerabilities that were exploited in that incident and how the consequences could have been better mitigated. Best practices of companies are adapting to the changing threat landscape and are thus evolving at a similar pace.

Public officials interviewed for this report perceived this challenge in surprisingly different ways. Some have acknowledged that their agencies' reflections on a more dynamic approach to standards and certificates are still in their infancy. Other interview partners seemed to be less concerned about the changing threat landscape. This might be due to their more objective-oriented approach. Cybersecurity objective generally remain the same even if the types of threats are changing. Objective-oriented approaches are often combined with more specific guidelines suggesting measures to achieve these objectives, but guidelines are usually policy instruments that are easier to adapt the changing types of threats than international standards and regulation.

2.2 Use of the term digital products

Since 2020, the Geneva Dialogue has focused on the security of so-called 'digital products.' Similarly, other international policy initiatives also increasingly focused on this area.[12] Finally, domestic legislative acts or executive orders mandating public agencies to develop policies or programs equally use the term 'digital products'. However, in general the term is not used in legislation or policies that determine concrete security objectives and measures (normative instruments on the operational level).

To better understand this landscape and the appropriate use of the term 'digital products', this section outlines the understanding and use of the term by different stakeholders and within different contexts. The usage of this term matters because it indicates the different stakeholders and industries that should be involved in the discussion and this is relevant for the agenda setting of specific meetings.

2.2.1 Geneva Dialogue partners – a broad understanding

During a workshop of the Geneva Dialogue in June 2021, participants showed a very broad understanding of the term 'digital products.'[13] According to the contributors, a digital product is any type of software, hardware or combination thereof (also called an integrated system). This definition may be influenced by the traditional distinction of security engineers between those who work on hardware, software and network security. Integrated systems are added to this list because the combination of soft- and hardware creates new threats and requires different security practices.

[12] Sometimes the term ICT products and services is used. Here, the term ICT products is considered to be same than digital products.
[13] Participants included industry representatives and academics collaborating with the Geneva Dialogue.

The participants of the Geneva Dialogue workshop discussed a comprehensive understanding of digital products based on an excerpt of the OECD Draft Recommendation on the Digital Security of Products. There are a number of elements that might characterize digital products that were discussed during the workshop, including the ability of the product to connect to a network; the handling, processing or exchange of data; and/ or the existence of code.

2.2.2 Initiatives and legislative documents using the term digital products

A number of private sector and multi-stakeholder initiatives also use the term 'digital products.' Most of these international initiatives that emerged in 2018 focus on particular aspects of strengthening the security of digital products.

The Paris Call for Trust and Security in Cyberspace, for example, encourages states to cooperate with private sector partners, academia and civil society to "strengthen the security throughout the products lifecycle and supply chain."[14] The signatories of the Cybersecurity Tech Accord commit to protect against "tampering with and exploitation of technology products and services during their development, design, distribution and use."[15] Finally, the report of the Global Commission on the Stability of Cyberspace highlights the need to "take reasonable steps to ensure that [...] products and services are free from significant vulnerabilities", and to "take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process."[16]

In contrast, the Geneva Dialogue is not limited to any particular facet of the security of digital products. This approach is similar to the Charter of Trust, initiated by Siemens, which calls broadly upon signatories of the Charter to "adopt the highest appropriate level of security."[17] When reflecting on the agenda of such comprehensive initiatives, it seems even more important to have a clear understanding about the meaning of digital products, whether there are common issues relevant for all types of digital products and what differences might exist between different products and services.

Finally, 'digital product' is also used in a number of domestic documents mandating particular agencies to develop policies or proposals (legislative mandates).

> **Example:** The EU regulation 2019/881 introducing the EU Cybersecurity Certification Framework uses the terms of "ICT products, ICT services and ICT processes."[18] In addition, the more recently adopted U.S. Executive Order on Improving the Nation's Cybersecurity refers to "software products and services."[19]

Legislative documents mandating particular agencies should be distinguished from legislative acts and guidelines that establish security objectives and propose concrete measures to achieve these objectives (normative instruments on the operational level).

[14] Paris Call for Trust and Security in Cyberspace (2018) Principle 6.
[15] Cybersecurity Tech Accord (2018) 'Commitment 2'.
[16] Global Commission on the Stability of Cyberspace 'Advancing Cyberstability – Final Report' (2019) Proposed Norm 6.
[17] Charter of Trust (2018) Principle 3 "Security-by-default".
[18] EU regulation 2019/881 (2019).
[19] United States White House 'Executive Order on Improving the Nation's Cybersecurity (14028)' (2021).

2.2.3 Normative instruments on the operational level

Legislative acts and guidelines on the operational level rarely use the term 'digital products.' Most legislative acts (on the operational level) distinguish between different types of technologies. The majority of jurisdictions analyzed for this report, for example, have specific guidelines or legislation in place addressing the security of IoT devices, cloud computing and 5G technologies. In some jurisdictions, public policymakers are also considering security standards for managed service providers and Software as a Service (SaaS) providers though the conversation regarding these measures is still in its infancy.

> **Example:** The European Union Agency for Cybersecurity (ENISA) has been mandated "to support and promote the development and implementation of a cybersecurity certification of ICT products, ICT services and ICT processes." This shall, however, be done by "preparing candidate European cybersecurity certification schemes."[20] These candidate schemes may refer to a specific type of technology, for example, a cybersecurity certification scheme on cloud services.[21]

In addition to the technological distinctions, most jurisdictions are considering the development of guidelines or legislation for specific use cases of products. A great number of jurisdictions, for example, are currently developing or implementing governmental measures addressing the security of consumer IoT devices.[22] In other jurisdictions. There are highly specialized security requirements for specific products like digital IDs or smart electricity meters.

There are only a few normative documents on the operational level using the term 'digital products', but if they do, they are limited in other aspects. The U.S. NIST Supply Chain Risk Management Practices for Federal Information Systems and Organizations[23], for example, addresses software products and services but it is limited to the cross-cutting issue of supply chain risks in the context of governmental use of these products and services.

Figure 1: Reference to digital products by normative documents on the operational level

generally no, scope of documents limited to...

- type of technology: IoT devices, cloud computing, 5G, AI systems
- type of provided service: managed service providers, etc.
- specific end user, e.g.: consumer IoT
- specific use case scenario, e.g. IoT toys, digital IDs, smart electricity meters

yes, but only if limited to particular security aspect and/ or end user

- e.g. only addressing supply chain risks for governments entitites as end users

In addition, the analysis reveals that documents tend to avoid the term 'digital products' if the policy or regulatory instrument might evolve into mandatory legal requirements for developers, vendors or other stakeholders. In documents outlining policy intentions and general principles, 'digital products' might still be a useful term. However, the impact of international discussions on matters of digital product security would

[20] Art. 8 EU regulation 2019/881 (2019).

[21] ENISA 'EUCS Cloud Service Scheme – EUCS, a candidate cybersecurity certification scheme for cloud services' (2020).

[22] For more details about governmental programs addressing the security of consumer IoT, see annex.

[23] NIST 'Supply Chain Risk Management Practices for Federal Information Systems and Organizations' (2015).

increase if participants distinguish between general principles for all types of digital products and norms that are only relevant in the context of certain technologies.

Distinction between services and products

Finally, there is a debate whether regulations and policies aiming to strengthen security should (continue to) distinguish between digital products and services. This distinction stem from contract law, where only the provider of a service has an ongoing obligation for a determined period. The seller of a product, in contrast, generally fulfills all obligation upon delivery of an adequate product. On the one hand, this distinction has in the digital space since developers of products now frequently have obligations to maintain and update their product until the end of its lifecycle. On the other hand, industry partners of the Geneva Dialogue workshop confirmed that different policies are used internally for products and services.

International and domestic policy documents regularly refer to digital products and services in the same sentence. Sometimes any distinction between digital products and services is completely abandoned. In particular, international state-led conferences and departments within some state agencies regularly use generic terms, including "digital technologies" or "advanced technologies" when referring to different types of digital products and services.

In the end, the distinction between digital products and services might be most relevant for determining whether they should governed as critical infrastructure. The introduction of the EU Network and Information Security Directive (NIS Directive) distinguishes between digital service providers and developers of hardware and software products with the argument that the latter "are already subject to existing rules of product liability."[24] In contrast, digital service providers are not subject to existing rules and thus are governed by the NIS Directive[25].

2.2.4 Potential implications for future policy dialogues

Whether a distinction between products and services is required to move forward with concrete recommendations is debatable. It seems that this distinction is inherently linked with concurrent legal obligations in each respective jurisdiction. When considered in the context of international policy, existing distinctions between products and services may not prove helpful nor instructive. Ultimately, the distinction does not contribute to the objective of understanding and identifying common ground between jurisdictions, and thus it should not be considered of key relevance for international policy discussions.

Whether the Geneva Dialogue and similar fora should continue discussions about the security of digital products or pursue different discussions about the security of different technologies and use cases depends on the objective of the policy forum. The ultimate questions that need to be asked are:

- Should we have horizontal security standards that are applicable to all types of existing and emerging technologies?
- Can we formulate such horizontal standards in a way that they effectively increase the security of products?

[24] EU Directive concerning measures for a high common level of security of network and information systems across the Union (EU NIS Directive 2016/1148) (07/2016) introduction para. 50.

[25] Digital service providers are defined by the NIS Directive to be 'essential service providers', which can be understood as roughly synonymous with 'critical infrastructure providers' used in other jurisdictions.

Some stakeholders, particularly from industry, argue in favor of horizontal standards for all types of digital products.[26] These actors highlight the risks of fragmented regulation as well as the increased complexity of the regulatory environment. In the view of these stakeholders, overly complex regulations will ultimately hinder the goal of increasing security. If different regulators adopt different standards for each type of technology or use case, this will increase the administrative and legal burden on companies but it will not necessarily support companies in improving their security practices.

Another argument in favor of horizontal security requirements is the interdependence between different types of digital products. For example, IoT applications are using different types of software and the data are often stored in the cloud. In addition, there are crosscutting issues that are relevant for more than one digital product (e.g., supply chain security or vulnerability disclosure processes).

There are, however, also good arguments to discuss standards and policies for each different type of technology separately. The OECD analysis paper finds that "digital security gaps may vary significantly across product categories."[27] Moreover, even crosscutting issues like supply chain security might have different challenges depending on the particular product.

> **Example**: One tool to improve supply chain security is to require a 'software bill of materials' from product developers. A bill of material is one centralized source of information listing all sub-products used for a broader product or service. In the case of an incident, a potential victim can react quicker if one immediately knows the components of the product that are in use. A recently published report by the US National Telecommunication and Information Administration (NTIA), however, highlights the challenges surrounding the transfer of 'software bills of materials' to the cloud context.[28]

To conclude, there are good arguments for and against addressing the security of digital products through horizontal security requirements versus developing different requirements for each type of technology. The result of this decision is relevant for a number of factors, including the stakeholders that should participate in the discussion and the level of detail that we can expect. A combination of both approaches might also be an option. There could be general international principles applicable to all types of digital products that would guide the behavior of states and companies in this context. These principles could be complemented by international or domestic requirements addressing specific technologies and thus being more precise about security objectives and measures.

> **Example:** The OECD policy paper discussion on the digital security of products develops high-level principles to address different types of identified challenges. "To address information asymmetries, there is a need to increase transparency and information sharing. To (...) realign market incentives, it is key to ensure responsibility and duty of care for supply-side actors (...). To take into account complexity, there is a need to address digital security with proportionality, through a risk-based approach."[29]

[26] Digital Europe 'Setting the standard: How to secure the Internet of Things' (09/2021): Calling for horizontal legislation of all connected products because 70% of baseline cybersecurity requirements are already common across all connected products.
[27] OECD analysis 'Understanding the digital security of products: an in-depth analysis' (2021) p. 52.
[28] U.S. Department of Commerce, NTIA 'The Minimum Elements For a Software Bill of Materials (SBOM) pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity' (07/2021) p. 15.
[29] OECD 'Enhancing the digital security of products - a policy discussion', p. 16.

3 Legal dimensions

As outlined in the preceding section, legislation or public guidelines establishing concrete security requirements tend not to use the term 'digital products.' The term is typically used in policy instruments and in some legislative acts mandating public agencies to develop policies. Any clarification of legal responsibility requires a different, more concrete vocabulary. There are, however, legislative instruments and proposals specifically addressing the security of IoT devices, software, cloud services, 5G and AI technologies.

In addition, the variety of rules within different legal fields shapes the responsibilities of manufacturers, software developers and service providers. Some might argue that contract or insurance laws are the major force shaping digital product providers' decisions to improve their security practices. Others might expect that the behavior is mainly influenced by administrative or consumer protection rules. While there are many legal fields influencing security practices, there seems to be agreement among policymakers that the security of digital products is a new field of governance.

3.1 The idea of a new field of governance and regulation

Most jurisdictions have identified the security of digital products as a new field of governance and regulation. On the one hand, this field addresses security aspects from a different angle. On the other hand, it has significant overlap with existing public policies addressing CIP and individual rights regarding personal data. States consider CIP to be part of their national security strategies and have developed a range of public policies over the past 25 years.[30] In addition, security of information technologies is addressed in data protection regimes. The OECD Guidelines on personal data protection from 1980 already established a principle that calls for "reasonable security safeguards"[31] and most data protection laws nowadays include provisions on data security.

In comparison to CIP and data security rules, the governance of digital product security is relatively new. Discussions about digital product security were spurred in part by a number of major global cyber incidents that did not fully correspond to existing regulatory regimes of CIP and individual rights. These incidents did not involve personal data and they had an impact on a broad number of businesses, both those classified as critical infrastructure providers and other private businesses. The immense scale of some of these global cyber incidents is seen to be a direct result of insufficient security measures of widely-used products.

[30] Collier, S. & Lakoff, A. 'The vulnerability of vital systems' in: Dunn Cavelty, M. & Kristensen, K. (2008) 'Securing 'the homeland': critical infrastructure, risk and (in)security', p. 17: Identifying the US Commission on Critical Infrastructure Protection formed in 1996 as a crucial moment for widespread policy discussions.

[31] OECD 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (September 23rds, 1980) para. 11: determining the security safeguards principle for personal data.

Case example – The Mirai botnet and its use for a DDoS attack (2016): The Mirai malware targeted IoT devices running on Linux.[32] The virus took control of devices that were only secured with a common use default password. Infected devices became part of a botnet and a malicious actor then used the botnet to operate Distributed Denial-of-Service attacks (DDoS). Among others, the DDoS attack targeted the Domain Names System service provider Dyn. This led to the temporary disruption of a number of Dyn's clients websites, including websites from the well-known companies GitHub, Twitter, Reddit, Netflix and Airbnb.

Case example – WannaCry ransomware (May 2017): The WannaCry ransomware used a vulnerability in two versions of Windows (Windows XP and Server 2003), which had reached their end-of-life and were no longer supported by Microsoft.[33] Even though Microsoft released an emergency update for these versions, despite no longer supporting the software, the WannaCry virus managed to infect computers in more than 150 countries. Many global businesses and organizations fell victim to WannaCry, including the UK National Health Service. It is estimated that Windows XP and Server 2003 were still used by over 100 million users at the time the WannaCry virus spread.

While aspects of product security are nothing new to security experts, it has only been picked up by international policy debates over the past three to four years. The following figure provides an overview of the key differences between existing regulatory fields and the legal policy debate about the security of digital products.

Figure 2: Public policy fields addressing aspects of security

Security of personal data	Protection of critical infrastructure	NEW: Security of digital products
• focus on protection of personal data if processed by third party • enforcement by individuals or public data protection agencies	• focus on threats to the organization • national security approach: public-private cooperation in sectors where functionality is considered an interest of national security	• focus on threats to the organization • national security approach: public-private cooperation in sectors where functionality is considered an interest of national security

[32] For more details, see: OECD analysis 'Understanding the digital security of products: an in-depth analysis' (2021) Box 4.2. The Mirai Botnet 2017, p. 44.

[33] For more details, see: OECD analysis 'Understanding the digital security of products: an in-depth analysis' Box 4.1 The WannaCry ransomware 2017, p. 42.

As a new field of governance, it is important that the security of digital products is distinguished from regulatory approaches to protect critical infrastructure (CI) providers. However, it can be a difficult task to sufficiently distinguish both regimes.

Both types of policies are typically developed by different divisions within the same ministry. Individuals interviewed for this report were often based in teams called the "economy and society" or "businesses and consumers." This reflects the common distinction of policies addressing security standards protecting businesses, consumers and society as distinct from policies that focus on national security interests.

While the categorization is useful to understand the different fora where issues of cybersecurity are discussed, it should be noted that there is also a significant overlap between data security, CI protection and digital product security. Data protection regimes and instruments of digital product security both aim to protect consumers. However, data protection regimes usually grant rights to individuals. Consumer protection mechanisms developed for the security of digital products in contrast may or may not do so. Consumers may, for example, simply be protected through the determination of standards that have the expectation of a reasonable consumer as a benchmark.

It is even more complicated to draw a clear line between CI protection and digital products security. Cloud services and 5G technologies, for example, may be considered a digital product and a critical infrastructure at the same time[34].

To conclude, public policies and legislation addressing the security of digital products are relatively new. However, existing governance and regulations can provide important guidance and potential solutions to the challenges arising from this new domain. This is reflected in the following section.

3.2 Common legal concepts and policy tools

The narrative about the regulation of security is often characterized as mandatory versus voluntary. Some argue that mandatory legal requirements are necessary to improve the security of products or services. Others believe that mandatory requirements encourage a compliance culture but does not improve security in a significant way. Mandatory requirements, according to this argument, are negatively affecting international commerce and voluntary standards should thus be the preferable public policy tool.

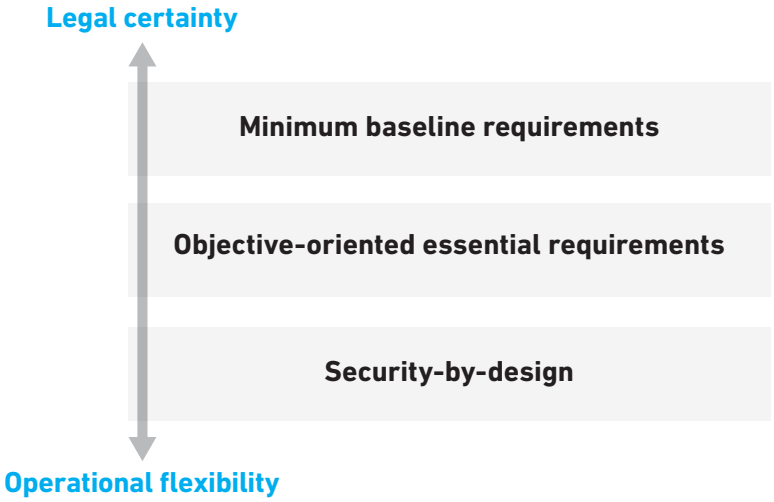
This report suggests a different narrative based on the depth of regulatory instruments. The research for this report has revealed that most jurisdictions are actually using a combination of mandatory and voluntary legal rules and standards. Different regulatory tools employ a variety of different legal concepts that range from providing legal certainty to more operational flexibility.

Regulatory instruments frequently use one or more of the following three legal concepts: (1) minimum baseline requirements, (2) objective-oriented essential requirements, and (3) security-by-design. Regulators and public policymakers will choose between these concepts depending on whether they consider legal certainty or operational flexibility more important in a given context. Legal certainty can be achieved through

[34] European Commission 'Proposal for a directive on measures for high common level of cybersecurity across the Union' (NIS directive 2.0): includes cloud services as essential entities of digital infrastructure.

the use of minimum baseline requirements. Comparatively, more operational flexibility can be supported through the use of more vague terminology, for example, the application of security-by-design. Security-by-design means that security aspects should be considered from the development phase throughout the entire lifecycle of a product[35].

Figure 3: Legal concepts aiming to strengthen the security of digital products



States have a number of reasons to use different approaches for different regulatory frameworks. Examples are included in the explanations below. The following analysis is primarily based on the examination of regulatory instruments addressing the security of IoT devices or software. Not all of this analysis can be translated to regulations or policies addressing the security of CI, including policies of specific technologies that might be categorized as a digital product and CI at the same time[36]. The main reason for this is that the concept of "security-by-design" is not relevant for policies and regulations of CI. Policies and regulation of CI protection traditionally address security practices of organizations and do not tackle secure development practices of products.

Minimum baseline requirements are functional requirements. They are usually more basic and compliance with these requirements can thus be easily assessed. In the context of consumer IoT devices, there are three functional requirements that can be assessed easily and could potentially be adapted as (mandatory or voluntary) minimum requirements by states. These baseline requirements are:

(1) no default passwords;
(2) an available procedure for vulnerability disclosures; and
(3) providing security updates during the entire lifecycle of a product[37]

[35] Commonly understood by the concept of "security-by-design."
[36] E.g. cloud services, 5G technologies and AI.
[37] ETSI 303 645 v.2.1.0 'Cyber Security for Consumer Internet of Things: Baseline Requirements' (2020): note that ETSI provisions are "primarily outcome-focused" (see introduction of the standard) but these first three requirements have been considered as minimum baseline requirements by a number of jurisdictions, including Australia, the United Kingdom and Singapore.

Objective-oriented essential requirements define concrete security objectives while leaving flexibility as to how the objectives may be achieved. Adequate measures to achieve the defined objectives may be found in standards or guidelines published by public agencies. There are many examples of regulatory instruments or public guidelines taking an objective-oriented approach. Objectives may be, for example, security measures

- to protect "the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their lifecycle[38]" or
- to be "reasonably resistant to basic attacks"[39]

The objectives might also be more concrete and limited ensuring, for example, that systems are resilient against outages.[40] These objective-oriented essential requirements can easily adapt to changing threat environments and provide security engineers with the flexibility to adopt the best security measure. At the same time, it is more difficult to run a conformity assessment. They might also contribute to more legal uncertainty. If non-conformity is combined with the possibility of a fine, courts might have to determine whether the adopted security measures were adequate according to existing guidelines and best practices.

Objective-oriented requirements are sometimes also called baseline requirements. In this context, the term 'baseline requirements' signals an attempt to find security measures applicable to a wide range of contexts while acknowledging that separate or additional requirements might be needed for particular domains or use cases.

> **Example:** ENISA developed baseline security requirements for IoT devices in 2017.[41] The objective of these baseline security measures is to be applicable to IoT devices used in critical information infrastructures. In addition, ENISA has also developed separate security requirements for particular domains, namely smart cars, hospitals, airports, cities and manufacturing.[42]

Finally, **security-by-design** means that products are developed with security threats in mind and that vulnerabilities are adequately addressed during the entire lifecycle of a product. The concept comes from data protection or privacy laws and is more frequently used in this context as opposed to digital products. Security-by-design is based on the assumption that, for a long time, security threats were not an issue during the development phase of software. An industry perspective about "security-by-design" was published in a good practice document of the Geneva Dialogue published in December 2020.[43]

The Singapore Labelling Scheme is one example using the concept of security-by-design for determining the security of digital products. However, here the concern is not necessarily the lack of security considerations in the design phase of products but rather the idea of a learning process.

[38] Regulation (EU) 2019/881 on information and communications technology cybersecurity certification (EU Cybersecurity Act) art. 46 (2).
[39] Singapore Labelling Scheme 'Minimum Test Specifications and Methodology for Tier 4' (2021).
[40] Australia Department of Home Affairs 'Voluntary Code of Practice - Securing the Internet of Things for Consumers' (2020) p. 6 (developing principles in accordance with ETSI standard 303 645).
[41] ENISA 'Baseline security IoT' (2017).
[42] ENISA 'Good practices for IoT and Smart Infrastructures Tool'.
[43] Geneva Dialogue of Responsible Behavior in Cyberspace 'Security of digital products and services: Reducing vulnerabilities and secure design – Industry Good Practices' (2020).

Example: Level 2 of the Singapore Labelling Scheme requires that products have been developed by using the principles of security-by-design.[44] Manufacturers of products can get a level 2 rating by self-assessment. The interview partners of the Cybersecurity Agency of Singapore (CSA) provided an example of a company who was advised to withdraw its level 2 rating application due to insufficient security practices. According to CSA, the idea of the level 2 rating is also to educate developers about security requirements so that they could adopt them in the version of their product.

Another concept that is used broadly in the regulation of specific technologies but also critical infrastructures is the concept of the "**state of the art.**"[45] Ideally, this concept captures the constant evolution of what is considered an adequate security measure for a particular protection objective; today's standards may not be adequate tomorrow.

Example: A particular length of an encryption key might be adequate today but with the constant evolution of computing power, new standards may mandate a longer key.

The precision of rules or standards should also be distinguished from the question of voluntary or mandatory requirements. It is sometimes argued that security requirements should be voluntary in order to be less intrusive into the market. However, mandatory requirements might not necessarily be the most intrusive tool. If the rules are kept as basic, functional requirements, they might be easier to implement and thus be less intrusive than initially expected. This would explain why some industry representatives have expressed an interest in mandatory requirements during domestic consultations of public guidelines and proposed legislation.[46]

[44] Ministry of Communications and Information, Cyber Security Agency 'Cybersecurity Labelling Scheme (CLS)'.
[45] See, for example, the German IT Security Law 2.0 (2021).
[46] Information is based on one of the interviews conducted for this report.

4 Fragmentation and international cooperation

The Geneva Dialogue industry partners raised concerns regarding whether legislators and regulatory agencies are equally concerned about the fragmentation of rules as the private sector. Based on the interviews conducted for this report, it appears the negative impacts of fragmentation are a consideration for public policymakers. In particular, the fact that mandatory security requirements are typically viewed as exceptional is perhaps evidence of that concern. Mandatory rules are often limited to specific products, such as electronic identification with governmental identity documents or medical devices.[47]

Example: The United Kingdom developed guidelines for consumer IoT devices as early as 2018.[48] Initially, the guidelines were intended to be voluntary. After public consultations of regulatory proposals, however, the respondents showed a preference for mandatory baseline security requirements. Despite this feedback, the UK government was concerned about the cost of such a regulatory intervention and commissioned two research reports to examine the issue.[49]

In general, the level of concern over fragmentation and the motivation to harmonize depends on the type of policy tool (technical standards, certification processes and labels).

4.1 Standards, certification processes and labels: domestic or international?

The three most important public policy tools to address the security of digital products are standards, certification and labels. The first step is always to define adequate security standards. Certification is the process to evaluate conformity with those standards. Finally, labels are the visual symbol indicating that a conformity assessment has been conducted. The purpose is primarily to provide transparency for the end user.

Figure 4: Public policy tools to address the security of digital products

The degree of harmonization is different depending on what tool is under discussion. Some standards are developed at an international level by standardization organizations.[50] Others are developed by national or regional organizations, for example, the United States National Institute of Standards and Technology (NIST) or the European Union Agency for Cybersecurity (ENISA). Frequently, national or regional guidelines are only voluntary and there is a strong effort by states to build upon existing standards and guidelines. In addition, states and industry are motivated to harmonize standards in order to avoid the creation of administrative burdens. Ideally, standards should not only avoid creating burdens but also be useful for the daily work of companies and in cooperation with contractual partners.

[47] See for example EU regulation (2017/745) on medical devices.
[48] UK Department for Digital, Culture, Media and Sport 'Code of Practice for Consumer IoT security' (2018).
[49] See 'Supporting research: Evidencing the cost of intervention' (2020) and the related 'Technical report' (2020).
[50] See for example: ETSI 303 645 v.2.1.0 'Cyber Security for Consumer Internet of Things: Baseline Requirements' (04/2020); IEEE 'Internet of Things (IoT) Security Best Practices' (02/2017).

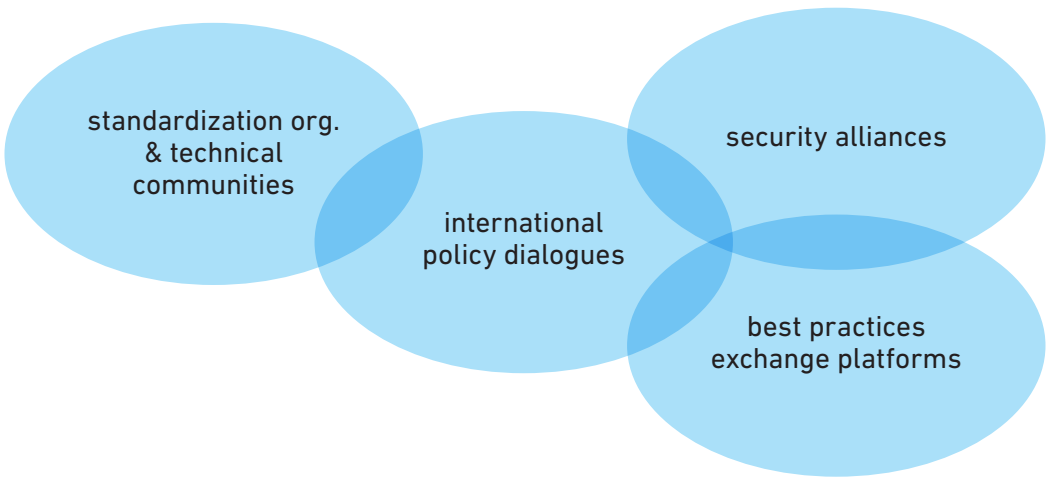
Regarding certification, harmonization is achieved through bilateral agreements between states that recognize both countries' domestic certification processes and authorities. Domestic authorities usually assess whether a product or entity complies with a particular set of standards. Most representatives interviewed for this report mentioned a number of bilateral agreements of this kind between their governments and other states. In the case of some certification regimes, it is also possible that domestically-authorized certification authorities issue an internationally-recognized certificate.[51] States are motivated to harmonize certification procedures in order to avoid market disruptions.

Finally, most labels are developed domestically. Despite this, many governments have an active exchange about the effectiveness of labels and share results of related research studies.[52] Some governmental agencies also lobby for the same use of assessment levels or standards across several jurisdictions. However, there is no attempt to unify different labels or to develop common assessments that can be used in a number of jurisdictions. There may also be good reasons to keep labels local, given that the consumer expectation and language varies between markets.

4.2 Existing fora for international cooperation

The author asked all public officials interviewed for this report whether they already have an exchange about regulatory challenges and potential solutions with public agencies in other jurisdictions. The interviews revealed that some states have recently created new fora and increased their exchange about public policy approaches towards digital product security. In addition, interviewees reported a number of new platforms that may prove important venues for future intergovernmental exchange. The different international fora discussing the security of digital products can be divided into the following four categories with overlaps of purpose between certain fora.

Figure 5: International fora for public policymakers to discuss security of digital products



[51] See, for example, products certified under the Common Criteria Arrangement.
[52] The representatives interviewed for this report highlighted sometimes even daily or weekly exchange with counterparts in other jurisdictions.

Many fora fall into more than one of the four category. The fora mentioned by the interview partners are thus all mentioned the following list without any distinction of their character:

- International Common Criteria Conference (ICCC)
- IEEE World Forum on the Internet of Things
- RSA Security Conference
- Cloud Security Alliance (CSA)
- Workshops organized by national agencies, e.g. NIST Workshop on Cybersecurity Labeling Programs for Consumers (09/2021)
- European Union/ ENISA
- Bilateral exchanges
- OECD Working Party on Security and Privacy in the Digital Economy (SDE)
- NATO
- G7
- Five Eyes Alliance: Statement of Intent regarding the security of the Internet of Things (07/2019)
- International Cybersecurity Conference – ONE Conference: organized by Dutch Ministry of Economic Affairs and Climate Policy, the National Cyber Security Centre and the Municipality in The Hague
- Quadrilateral Security Dialogue (Australia, India, Japan, United States): Working Group on Critical and Emerging Technology (see White House Fact Sheet (03/2021))
- Agile Nations Charter: recently created exchange platform about public policies between Canada, Denmark, Italy, Japan, Singapore, United Arab Emirates and United Kingdom

Despite this variety of existing fora, the majority of public policymakers expressed the desire for more opportunities for exchange about public policies. Many of these fora focus on the development of standards, and there are far fewer opportunities to discuss innovative policy approaches and regulations.

5 Future areas for policy research and key open questions

This report has provided a broad overview of public policy challenges and regulations aiming to strengthen the security of digital products. It did not analyze public policies or regulations addressing any specific technology. A more detailed analysis about public policies and regulations addressing the security of consumer IoT devices can be found in the annex. Public policies with regard to consumer IoT security are the most mature compared to policy solutions, for example, targeted toward cloud service security or security of AI technologies. It is likely that policy research and international dialogue regarding these technologies will intensify in the near future.

This analysis has revealed a number of questions. Addressing these questions would help develop better policies about the security of digital products. It might also help to identify areas where better international coordination is necessary. Finally, answers to these questions are crucial to identify the stakeholders that should be involved in future policy dialogues about the security of digital products.

Should security requirements be developed on a horizontal level for all digital products?

Chapter 2.2 of this report analyzed the use of the term 'digital products' by different international and domestic policy and regulatory instruments. It concludes legislative acts and public guidelines establishing security objectives and suggesting specific technical or organizational measures only use the term in exceptional circumstances. Most of these instruments concentrate on different types of technologies or particular use cases.[53]

Some stakeholders, particularly from industry, would prefer to see more policy and regulatory documents developing horizontal security requirements applicable to all types of digital products and use cases. In their view, specific requirements should then only be established where deemed necessary.

To make real progress on digital products security in international policy dialogues, it will be necessary to carefully assess the benefits and downsides of developing horizontal security requirements. What might such horizontal requirements look like? Is it even possible to develop horizontal standards that would meaningfully and effectively increase the security of products?

Is it possible to address the security of digital products on a truly global level?

The aspiration of the Geneva Dialogue is to engage in a dialogue with leading businesses to contribute to global policy processes. This has included organizations headquartered in many different jurisdictions around the world. Yet, when it comes to public policies and regulatory tools, it remains to be seen whether a truly global policy debate is feasible.

While government agencies from all major global actors participate in standardization efforts, most exchanges on a policy and regulatory level take place among a limited number of states. The interviews conducted for this report have shown that these policy debates and exchanges often occur within long-established

[53] See 2.2.3.

organizations or security alliances.[54] In addition, the author of the report was unable to connect with public authorities of states that are not part of these existing international networks. Attempts to discuss domestic public policy approaches were made through academic, diplomatic and industry channels. One explanation for the lack of engagement might be a different understanding about the role of academia and think tanks but it may also be that the term 'digital products' is not used with certain jurisdictions.[55]

What are the limits of regulatory interventions?

Chapter 3.2 of the report elaborated on the different legal concepts frequently used in policy or regulatory documents aiming to strengthen the security of digital products. Recurring questions include how effective are standards or rules in improving security and what are the negative impacts on the market. Ultimately, the legal contexts and concepts most discussed all seek to shed light on the same challenges outlined at the beginning of the report[56]: (1) the potential for market disruption due to mandatory security requirements, (2) making software and product developers care about voluntary instruments and (3) how to adapt policy and regulatory tools quickly enough to changing threat environments. An international debate and exchange about these challenges, and potential solutions, can make it easier to develop policies that are effective without negatively impacting the market.

In which areas should harmonization efforts be increased?

Finally, the report highlighted that the task of harmonizing policies and regulatory approaches differs across the tools of standardization, certification and labels.[57] While there are efforts to coordinate the development of standards on an international level, many standards are still developed on a domestic and regional level. It is even more unclear which standards may potentially be made mandatory by domestic regulatory agencies. Interviewees of this report have highlighted their concerns and efforts to develop their own standards according to international practices and to increase mutual recognitions of certifications. However, the risk of fragmentation and its negative consequences for the economy remain an ongoing concern.

[54] See 4.2.

[55] Some public officials, for example, interpreted the "security of digital product" as IoT security. Their understanding generally did not include policies addressing the security of cloud services, 5G or AI technologies.

[56] See 2.1.

[57] See 4.1.

6 Annex: Certificates and labels for consumer IoT devices

The objective of this report was to provide an overview of public policies and regulatory instruments addressing the security of digital products. Insights about policies addressing only IoT security would have been outside the scope of the report. However, many public officials interviewed for this report provided insights into their policies on consumer IoT security. The perspectives provided during these interviews are shared in this annex.

Reflections about certificates and labels for consumer IoT devices are arguably the most mature public policies among all categories of digital products. Yet, some jurisdictions are still at the beginning of developing policies or legislation that addresses the security of consumer IoT devices. The following paragraphs reflect how other jurisdictions have addressed the topic and the aspects that they have studied and reflected upon.

Step 1: Voluntary guidelines

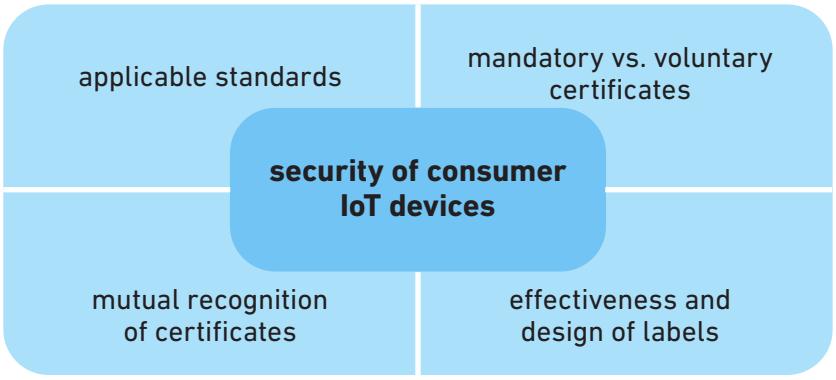
Many jurisdictions start their regulatory process by developing voluntary guidelines for consumer IoT devices. It often serves as the starting point for governments to engage in dialogue with relevant stakeholders from industry to subject matter experts. Voluntary guidelines are typically published after widespread public consultation and workshops.

Examples: UK Code of Practice for Consumer IoT Security (2018), US NIST Cybersecurity for IoT program - NISTIR 8259 Recommendations for IoT Device Manufacturers (2020), Australia's Voluntary Code of Practice for Consumer IoT (2020), India's Code of Practice for Securing Consumer IoT (2021).

Step 2: Certification and Labelling Schemes

Once a jurisdiction has published voluntary guidelines, many jurisdictions begin discussions about establishing certification and labelling schemes. Some key aspects that are typically considered include: (1) the applicable standard, (2) whether a particular certificate shall be mandatory, (3) bilateral agreements to recognize domestic certificates and (4) the effectiveness and design of labels.

Figure 6: Typical aspects to consider by regulators and public policymakers



Some jurisdictions apply international standards or parts of them directly, some use international standards to develop their own domestic technical or organizational standards. In the context of consumer IoT devices, the ETSI standards 303 645 are frequently applied. Though these standards contain thirteen different measures, not all jurisdictions make use of all the described measures in the same manner. Singapore, for example, only uses the first three measures in order to assess the most basic level of security. Similarly, consultations about mandatory requirements in the UK and Australia also use the first three measures, while including all thirteen standards in their voluntary guidelines.

Closely connected is the question of how conformity with standards should be assessed. The possibilities range from self-assessments to authorized private organizations or an assessment by state agencies. Certification of consumer IoT devices is generally voluntary, but some jurisdictions have made the certification of specific products mandatory.[58] A common feature among jurisdictions is to certify different levels of security maturity of a product[59]. A mandatory certification may thus be less intrusive than it seems at first glance, if the level of certified maturity is very low.

If a certification scheme is to be established, the question of mutual recognition between different nation states necessarily arises. While mutual recognition agreements are typically only adopted after a national certification scheme is in place, it makes sense to reflect on potential obstacles to recognition even as early as during the development phase of the certification scheme.

Finally, public policymakers working on consumer IoT security frequently reflect on the adoption of labels. Some stakeholders are skeptical about the effectiveness of labels. The UK[60], Singapore[61] and Australia[62] have conducted or are conducting studies to examine whether consumers are influenced by security labels. Those studies that have been completed indicate that labels are influential over the behavior of consumers. In addition, a label can contribute to greater transparency about security practices, leading to easier examination by security researchers or public agencies.

[58] Singapore has made the certification of home routers mandatory. Within the EU, there are discussions to develop mandatory certification schemes.
[59] Security maturity refers to the potential evolution of a product – initially focusing on getting it onto the market as quick as possible with only minimal security features and adopting more sophisticated security features over time.
[60] J. Stannard, R. Writer-Davies, D. Spielman, J. Nurse 'Consumer attitudes towards IoT Security' Report commissioned by UK Department for Digital, Culture, Media and Sport (December 2020).
[61] Unpublished survey, shared with the author.
[62] Study in progress.

One critique of labels is that they are only capturing the security posture of a product at the moment of the conformity assessment. In addition, labels usually differ between jurisdictions and there are practical concerns regarding the number of labels that can be displayed on one single product. Proposed solutions include 'dynamic labels', for example, a QR code providing the ability to look up the most recent updates and the level of security at any given time. Such a feature is similar to information on our cellphones about the software version used on the given device and potentially required updates.

Step 3: Other measures to avoid a market for insecure products

Finally, legislators and public policymakers may want to consider whether additional measures are necessary in order to avoid a market of insecure products. If certification and labelling schemes are established only on a voluntary basis, security then becomes a feature of a product. However, it is reasonable to assume consumers will expect that any product on the market comply with a certain minimum level of security. In addition, some security risks do not pose a threat to the consumer of the product but to third parties who were not involved in the purchase of the product.[63] In this case, the level of security is likely not sufficiently important when purchasing the product.

There are currently two main approaches to address the security of uncertified products. One is to change the rules of product liability.[64] A product developer might be made liable if a cyber incident causes harm that could have been avoided if the developer had implemented reasonable security practices. Another approach is to require mandatory baseline security requirements for any consumer IoT device on the market. The UK Department for Digital, Culture, Media & Sport is currently working on such a legislative proposal, which is expected to be introduced into Parliament no later than spring 2022.

[63] A clear example of this phenomenon is the Mirai botnet DDoS attack on Dyn, which used consumer IoT devices to target a third party.
[64] See suggestion by the US Solarium Commission.