GENEVA
DIALOGUE
ON RESPONSIBLE
BEHAVIOUR
IN CYBERSPACE

*Online event*

# ‘Security of digital products and the regulatory environment’

29 September 2021

## Report and messages

## Context

The fast-changing technological environment introduces great security challenges. The threat landscape is continuously evolving, with a growing sophistication in techniques, tactics, and procedures being employed by malicious actors, including the well-resourced advanced persistent threat (APT) groups. The high socio-economic and political impact of cyberattacks increasingly compels states to devise legal and regulatory measures for bolstering the security of digital products. National regulators around the world are developing various models to address those concerns, the example of such being product certification and labelling schemes.

The urgency with which these measures are being conceived has led to new regulatory efforts remaining out of sync with each other. Furthermore, the broad range of international standards makes it difficult for regulators to base their work on common and mutually endorsed criteria and guidelines. This poses an obstacle for businesses in complying with different baseline requirements across various jurisdictions, while at the same time addressing the market-driven demands and standards for product security. Governments need to move faster and catch up with the pace of technology, while finding ways to interact with important stakeholders that lead digital transformation. There is a need for greater dialogue and aligning national regulations more closely with industry good practices, international standards, and global norms and principles. This event addressed the related challenges and opportunities.

## The event

Geneva Dialogue on Responsible Behaviour in Cyberspace (Geneva Dialogue) initiated a series of online discussions between the industry, standard-setting organisations, diplomats, and regulators, about the future of norms, regulation, and standardisation for the enhanced security of digital products.

The second such discussion, 'Security of digital products and the regulatory environment', took place on 29 September 2021. Representatives of national regulators, government officials, companies, standardisation organisations and technical communities, and research and academic community from around the world, contributed to the discussion (list of participating organisations can be found in the Annex).

The 3.5-hour long event consisted of five segments:

1. High-level remarks and setting the stage: 'Regulating security of digital products: trends and challenges'

Keynotes were provided by high-level representatives of the governments and regulators:

- Ms Livia Leu, State Secretary, Federal Department of Foreign Affairs, Switzerland
- Dr Stanislav Raščan, State Secretary, Ministry of Foreign Affairs, Slovenia, on behalf of the Presidency of the EU
- Mr Gaurav Keerthi, Deputy Chief Executive, Cyber Security Agency, Singapore

This session also hosted 'Setting the stage' panellists:

- Dr Bushra Al Blooshi, Head of Research and Innovation, Dubai Electronic Security Center, UAE
- Mr Peter Stephens, Head of Secure by Design Cyber Security, Department for Digital, Culture, Media & Sports (DCMS), UK
- Ms Angela Smith, Computer Security Division, Department of Commerce's National Institute of Standards and Technology (NIST), USA [tbc]

Session was moderated by Dr Maya Bundt, Head Cyber and Digital Solutions, Swiss Re Reinsurance. Keynotes provided directions and trends related to security of digital products on a strategic level, including insights into other ideas/plans and strategic thinking. The discussion which followed outlined the work of some of the national regulatory authorities in the field of security of digital products, and ways of addressing the main challenges of the fast-changing environment.

2. Presentation of research results: ‘Security of digital products: regulatory approaches, challenges, and limits’

Ms Nele Achten, Senior Researcher for Cyber Security and Foreign Policy, ETHZ Center for Security Studies, presented the preliminary findings of the research that maps the challenges public policymakers face in this context, and the solutions that have been adopted.

3. Focused Discussion 1: ‘Challenges and effects of the emerging regulatory environment’

The open discussion, moderated by Ms Anastasiya Kazakova, Senior Public Affairs Manager, Kaspersky, mapped the main challenges related to national regulatory frameworks, gaps between them, and places in which dialogue does not exist and could be facilitated.

4. Focused Discussion 2: ‘Addressing the regulatory challenges related to security of digital products’

This session, moderated by Mr Seán Doyle, Lead, World Economic Forum Centre for Cybersecurity, discussed ways to address the mapped challenges, and facilitate the dialogue where it is not existing (or not sufficient), and explored the role of the Geneva Dialogue and other fora.

5. Takeaways and closing

The closing session with Dr Jovan Kurbalija, Head, Geneva Internet Platform, provided key takeaways and possible further steps for this discussion.

The event concluded with an informal networking in a virtual cafeteria.

## Key messages

1. The security of digital products is an emerging field of regulation. To set the efficient, agile, and harmonised regulatory environment that will reduce vulnerabilities, national regulatory frameworks should lean upon the global norms and principles, international standards, and good industry practices. **More dialogue between leading producers and vendors of digital products and regulators, diplomats, standardisation and technical community is needed – on the national and international level.**
2. Certain basic building blocks for regulatory frameworks are already in place. To support further coordination and harmonisation, **it is necessary to clearly map what these building blocks are, and what the areas in which the emerging regulatory frameworks already align are, and accordingly outline the areas in which harmonisation should be enhanced**. The research under the Geneva Dialogue, conducted by the ETHZ CSS, related to governance approaches to the security of digital products, is a step in that direction.

3. It is evident that international negotiations about the framework of responsible state behaviour in cyberspace takes into consideration the risks stemming from exploiting vulnerabilities in digital products, and deems appropriate to outline certain measures to reduce such vulnerabilities. To assist regulators in incorporating those high-level norms and principles, **further discussion is needed on how international security in digital space connects with the digital security of internationally used products**.
4. Several multilateral and multistakeholder venues which cover, directly or indirectly, security of digital products exist. There is a need, however, for a venue for direct dialogue among the regulators and authorities in charge from various countries, along with diplomats, industries, standardisation and technical communities. Building on the adage that emerged at the May event "All cyber-roads lead to Geneva", **Geneva may provide *good offices* for a global summit on the security of digital products**.
5. Enhanced dialogue will further clarify main challenges, building blocks, and good and bad practices. This will allow for **developing a comprehensive capacity building programme on the security of digital products**, to better prepare public institutions and national authorities, as well as the industry, technical community, and other stakeholders to contribute to developing national frameworks, and to the emerging international dialogue.

## Findings

Key messages were prepared based on the discussions and the exchange among the representatives of regulators, industry, diplomats, standardisation organisations, and other stakeholders present at the event. Therefore, they should rather be perceived as fertile ground for further discussions, than as evidence-based research. In this regard, those messages should be used as a living document, open for comments.

The messages by no means represent the official positions of either of the participating institutions, the Geneva Dialogue hosts or partners, or the Geneva Internet Platform team that prepared this report.

### 1. Terminology: What are we talking about

#### Understanding of term(s)

To clarify the scope of discussions, Geneva Dialogue offers an understanding of the term 'digital products':

*Digital products include software, hardware, or their combination. They are characterised by (i) containing code; (ii) ability to process data; or (iii) ability to communicate/interconnect.*

Research conducted by the ETHZ CSS for the Geneva Dialogue, which examines the emerging regulatory trends related to security of digital products, revealed that the term 'digital or ICT products' is only used within high-level policy documents and legal instruments which mandate national agencies to develop adequate policies. Normative instruments on the operational level (legislative acts and guidelines that establish security objectives and propose concrete measures to achieve these objectives), however, distinguish between different types of technologies. They distinguish, for example, between policies and security requirements for consumer IoT devices, cloud services or AI systems.

In this regard, the use of the term 'digital product' seems to better suit those products that are digital in nature, than those that are both digital and physical - like IoT devices - which have specific risks and approaches to risk mitigation. One alternative suggested is the term 'digital security of products', since 'product' is more overarching and doesn't not need to be specifically defined. Still, this term would again refer to risks related to software, hardware, and combination thereof.

### Turning to 'digital'

Importantly, there is an emerging shift in understanding the 'security' part of the term as well. In most cases, the term 'digital' is being used (either as 'digital security of products' or 'security of digital products'), signalling a departure from the traditional 'cybersecurity' framing. There are few possible benefits of using 'digital' in policy processes related to security of products:

1. Unlike 'cyber', which is commonly linked to security and risks and used by security communities, 'digital' is typically used in the context of progress and opportunities. This allows blending the issue more easily into the opportunities-driven framing of digitalisation and development, familiar to the industry and the policy-makers.
2. 'Digital' also introduces a different focus: it refers to the economic and social aspects of cyberspace, as opposed to international security, defence, and crime aspects. It could, therefore, more easily be connected to the development agenda as well.

## 2. Regulatory approaches

### Framing

Security of digital products is a regulatory field in the making, and framing on the national level differs from country to country. Policy makers address these challenges through policies related to:

- *Critical infrastructure (CI) protection*: Most policies for CI providers focus on best practices to strengthen the resilience of the organisation, which include procurement control, implementing standards, etc.
- *Consumer safety*: Digital products are becoming integral parts of industries which already have strong safety regulations, like the health sector. It is important to note,

however, that existing safety regulation is not best adept for the security of digital products, because it presents a different composure of risk.

- *Security of digital products* (or, sometimes more specifically, the *IoT security*): Emerging rules addressing the security of digital products focus on security measures during the development and lifecycle of the product, through product labelling and certification schemes, among others.
- *Supply chain security*: Due to political and strategic interests, countries are considering regulations related to the supply chain, particularly to 5G technologies (though not limited to).
- *Data regulations*: Similarly, countries are addressing the issues of data processing, protection, and security, which then impacts the security of digital products as well.

### Voluntary vs mandatory?

Having in mind that secure digital products create a more secure digital infrastructure, one of the main dilemmas is whether voluntary mechanisms and incentives are sufficient, or mandatory ones are needed as well.

A general agreement seems to be that **voluntary approaches should dominate, to allow operational flexibility for vendors to embrace security by design**. Voluntary measures would stimulate a dialogue between the government and industry to promote digital products security, while not being perceived as an interference within the market activity. They would be specific and descriptive (e.g. setting minimum baseline requirements), and thus easy to implement and control.

Yet, **certain mandatory measures and regulatory mechanisms should, when necessary, also be put in place**, to ensure legal certainty and compliance. This particularly stands for more critical technologies, or technologies implemented in critical sectors.

A different regulatory approach might be needed depending on the types of products and industries:

- Certain digital products may be considered critical, and thus deserve specific attention. Those include elements of the operational technologies (OT), but also some general software or IoT which, if exploited, could cause more severe consequences (e.g. software that operates below the level of the operating system, has privileged access, or ubiquitous activity across the network).
- Some industries make a bigger impact on the overall security of our digital environment than others, and their responsibilities may be addressed differently. Large companies with innovation potential, competitiveness and market impact, and resources for releasing and maintaining compliant digital security products, should be approached differently than SMEs or start-ups producing non-critical products.

### Outcome-oriented principles-based regulations

Due to a fast-changing environment and specificities of different jurisdictions and markets within, it is advisable for regulators to focus firstly on *what* to do rather than on *how* it is done. Such **outcomes-oriented principles-based regulations** should:

- Define high-level guiding *principles* which are 'future-proofed'
- Set realistic and achievable *outcomes* (e.g. transparency, cooperation, duty of care)

These should be embedded into the regulatory environment, yet without technical specifications and measures, to avoid 'insecurity by compliance' (as standards and other technical approaches become obsolete). Guiding principles and desired outcomes could allow horizontal coverage across industries, and facilitate dialogue and learning between the industry and the public agencies, and finding a common ground within cross-border dialogue.

Principles include, among others:

- Protecting the public interest
- Risk-based approach to formulating policies
- Preserving dynamism of tech developments and innovations
- Encouraging harmonisation (or interoperability) of security approaches
- Holistic approach across the entire product lifecycle (and beyond it)
- Comprehensive approach, targeting both the producers to secure their products, and the users to know which security features are in place.

Further, principles and outcomes should be turned into technical means and specifications to reach these outcomes, but in accordance with their own needs, local culture and preferences, capacities and expertise, resources, governance model, etc. In this, regulators should preserve **flexibility** to change and adjust measures, as well as add new requirements or update means based on technological developments, emerging risks, and implementation challenges. Such specifications could serve as mere guidance to the industry, which would be allowed to find its own ways to achieve the outcomes, while competition may bring about innovative approaches.

### Baseline requirements

**Of particular importance is defining minimum baseline security requirements for security of digital products.** While baselines could be set as legal requirements for certain types of producers and products, ideally, they should be voluntary measures (at first). They should set expectations, and provide clearer guidance for developers on what to do. In order to avoid implementation turning into a complex process, however, baselines should attempt not to increase development costs (which is especially of relevance for SMEs and start-ups), and offer benefits for followers.

### Voluntary labels

One of the regulatory practices which is becoming prevalent is introducing voluntary labelling of products' security (akin to labels for energy efficiency of electrically powered products). Labelling schemes rely on cooperation between the industry and the government. **By helping consumers make an informed purchasing decision, labelling schemes drive a demand for secure products, and thus turn security into product's feature**. Notable examples are those from Singapore, UK, and the US.

There are, however, certain traps of the labelling schemes that regulators should watch out for:

- Safer products can be more expensive to develop, and labelling schemes should come with financial incentives.
- There are limitations of branding, as customers are primarily motivated by price; thus, awareness raising among customers should go hand-in-hand with labelling.
- Labelling might create a false sense of security, since customers are likely to perceive 'five stars product' as a perfect protection, thus disengaging from cyber hygiene.
- In addition, buyers with lower buying power would remain vulnerable, and the wide digital divide could result in widening the cybersecurity divide as well.
- Not much is known about the effectiveness of labelling initiatives yet, and close monitoring of effectiveness should be undertaken.

### Broad set of policy measures

**Regulators need to make sure that the tools and capabilities are in place** so that the industry and other institutions and organisations are equipped and capable to comply with requirements and improve security practices. This may include:

- Rewards and recognition from the government (e.g. Dubai excellence program);
- Guidance and training opportunities, especially for the small and medium enterprises (SME);
- Grant schemes, financial incentives, and assistance to companies (particularly SME) to adopt quality assurance schemes and invest in security by design;
- Stimulating business leaders to see secure products as a business case and a market advantage.

Yet, policy measures should go beyond those targeting the industry only, and should include:

- Preparing consumers through education and engagement, with simplifying the complex field of cybersecurity, and raising awareness about digital hygiene and maintenance;
- Developing competent labour market (e.g. security-by-design-ready software developers), in cooperation with the industry;
- Establishing national, and contributing to the development of international standards;
- Boosting international cooperation (by both public institutions and other sectors).

### Implementation

Regulatory environment should, of course, be accompanied with the implementation, evaluation, and feed-back mechanisms. Relying on compliance with widely accepted international standards not only contributes to implementation, but also allows interoperability. Yet, compliance alone is not sufficient any more.

Continuous risk assessment should be supported, along with the assessment of effectiveness of the introduced measures. An open and inclusive dialogue between regulators, industry, technical community, and other stakeholders plays an important role in collecting feedback and discussing improvements.

### Innovating regulations

**Regulatory environment and policy-making processes should become more agile and innovative**, in order to follow the pace of technological development. There are two notable fronts:

- *Engagement of the entire community*: Regulators should allow and manage consistent inputs from a wide variety of actors, through position papers, workshops, etc. (e.g. the engagement on the definition of critical software, requested by the US Executive Order 14028, Improving the Nation's Cybersecurity). This process should engage a variety of public authorities (those in charge of privacy and data protection, consumer protection, security, critical infrastructure, finances and economics, foreign affairs, etc.), industry associations (of vendors, banks, etc), research and academic organisations, and non-governmental organizations. Broad engagement, however, demands high responsiveness by the regulators, and thus increased resources and capabilities on their side.
- *Turning to dynamic documents*: While high-level principles and desired outcomes should remain future proofed, particular technical instruments should become 'living documents' (close to real-time) which could continuously be refreshed to incorporate comments and revisions (e.g. NIST Risk Management Framework, Security and Privacy Controls - SP 800-53). Certain elements of the traditional 'static' publications and guidelines should still be preserved, in order to accommodate the reality of bureaucratic and administrative formalities. In addition, the industry might face challenges in following and complying with an overly dynamic framework (even – or especially if – it is voluntary).

## 3. Roles of the industry

### Duty of care

Companies that create digital products must accept greater responsibility for the security of their products.

**At minimum, duty of care includes**:

- *security by design*, i.e. addressing risks from an early stage and throughout the product development lifecycle, including vulnerability treatment (coordinated vulnerability disclosure and vulnerability management processes);
- *security by default*, i.e. delivering the product preconfigured in a secure way;
- *security throughout the entire lifecycle*, and *responsible end-of-life*.

Regulators, in cooperation with the industry and other stakeholders, may define the elements more closely. Ideally, they should consult, or be in line with, the existing international policy documents and agreements, such as the OECD recommendations on digital security by the OECD Working Party on Security in the Digital Economy.

### Supply chain security

Digital products and systems are connected to one another. **Producers need to observe broader security of the supply chain**, not just the security of their products. In this regard, they also need to closely cooperate with each other.

Producers should observe various scenarios of how their products might be used (including being integrated into broader solutions, or as part of critical systems), and what risk they may create for such a use, and throughout the supply chain. Examples vary from pieces of code that become broadly used by producers (e.g. software libraries), to IoT devices that get integrated into operational technology and industrial systems. **Producers should also continuously assess the actual security of their products**, in context of the broader supply chain.

At the same time, relying on third-party components requires a mindset change which involves ‘zero trust’ posture, different design, continuous monitoring, etc. Besides, producers have to understand the risks of compromising a product, and be able to respond to such incidents.

### End-of-life, end-of-support, end-of-use

Three different, but connected, terms are important:

- *End-of-life* (EOL) commonly marks the date when sale or distribution of a particular product will be discontinued. Yet, not all producers understand it in the same way. In addition, users may interpret it from their own perspective, rather than from the perspective of providers.

- *End-of-support* (EOS) marks the date when the producer will discontinue providing support for the product, including issuing patches and fixes, and providing assistance. While it may be connected to EOL, EOS is a clearer signal of when the lifecycle ends from the perspective of the producer.
- *End-of-use* (EOU) is, on the other hand, linked to when users overall abandon the product. Since it is not set by the producers, it is much harder for regulators and providers to know how long the consumers might wish to use the product.

**There is a significant gap between the EOS and EOU of digital products**. In the case of IoT products, which have a shorter life cycle, this risks the emergence of the 'Internet of forgotten things'. In the case of software and code, which underpins all the critical systems of the society, the risks may be even higher.

**Producers should define the EOS responsibly to reduce the gap with the EOU**, and clearly and timely communicate the EOS to their customers. They should also consider and publicise options for post-EOS, for instance:

- Offer users to replace, upgrade, or migrate to a new version of the product (discussed in NIST SP 800-161 REV. 1);
- Open the source code and allow the broader community to take care of it, if interested;
- Where applicable, terminate the product and disable users from using the product further (though this may, in case of IoT and hardware, increase environmental concerns).

## 4. Harmonisation

### Avoiding fragmentation

As supply chain security becomes an increasingly important element of national security, and states turn to finding regulatory and policy solutions, there is a risk of industries starting to face a fragmented regulatory environment across jurisdictions. This would increase complexity of compliance, as well as costs to innovations, and would, in general, hurt the digital economy.

Particular policy and regulatory measures, such as certifications schemes and labels, are being discussed mainly in the domestic context, which allows addressing local concerns in a manner coherent with local culture and specificities. **It is, however, important that national regulatory frameworks lean upon the global norms and principles, international standards, and good industry practices.** This would allow them to be more easily harmonised and, where convenient, mutually recognised as part of bilateral or multilateral agreements.

*Global norms and principles* are being shaped in multiple fora. At the UN level, reports of the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) of 2021 provide voluntary norms and recommendations to member states, including those related to shaping the national regulatory framework in the context of securing the supply chain, avoiding the exploitation of vulnerabilities, and strengthening the security of digital products. Similarly, OECD, Paris Call for Trust and Security in Cyberspace, Charter of Trust, Cybersecurity Tech Accord, and other multilateral, multistakeholder, and industry venues set guiding principles.

Key *international standards*, developed by the ITU, ISO, IEC, IEEE, IETF, and other standardisation development organisations (SDO) and communities, are already internationally recognised and widely adopted by the leading industries. In general, those standards aim to build a common understanding across jurisdictions. Yet, the fast pace of technological development and its convergence (e.g. IoT with operational technology), ever-changing threat landscape, and increasing geopolitical relevance of standards, challenge the effectiveness of the existing standard-making and compliance processes, as outlined in the report from the Geneva Dialogue event on standardisation.

Industries continue to develop *good practices* to secure their digital products. A collection of good practices of some of the leading companies is available in the Geneva Dialogue report from 2020.

Decision-makers, regulators, industries, and other stakeholders should not only benefit from these fora, but also take active part in them.

### National standards and requirements

When developing national standards and requirements that underpin regulations, institutions should ensure interoperability of the developed technologies, and rely on the recognised international standards (e.g. ETSI EN 303-645 is broadly recognised for IoT consumer devices). At the same time, standards should be ‘consumable’ – accessible and user-friendly, to allow for an easier adoption.

Due to the challenges which international standardisation faces, it may happen that certain national standardisation organisations move faster than the international fora in some aspects (e.g. the US NIST leads international efforts in defining requirements for critical software, as results of its Presidential Executive Order). It is therefore important that national institutions and stakeholders take active participation in international standards discussions, in order to both follow the developments and feed their own experiences.

### Cross-border cooperation

To ensure interoperability of the developed technologies, and move towards better harmonised regulatory frameworks, broader cross-border and international cooperation is needed. While the industry, standardisation and tech communities, and other non-governmental actors already engage in various global venues, there is a need for greater involvement of decision-makers, regulators, national standardisation authorities, and other public institutions in cross-border dialogue on the security of digital products. A useful step is appointing a national contact point or authority in this field, which would receive a mandate to coordinate national efforts and international cooperation.

There are multiple options of cross-border agreements that could ensure harmonisation and recognition of regulatory mechanisms:

- Statements of intent (e.g. 'Statement of Intent regarding the security of the Internet of Things' from 2019 by Ministers of Interior, Homeland Security and Public Safety of Australia, Canada, New Zealand, the United Kingdom and the United States);
- Memorandum of Understanding and mutual recognition agreements (e.g. MoU between authorities of Singapore and Finland recognising both nations' cybersecurity IoT labels);
- Bilateral agreements (either thematic, or embedding security of digital products within the existing, broader ones);
- Creating multilateral, regional or international platforms to promote cross border recognition of cybersecurity certification.

It is, however, important to increase awareness among the regulators and policy-makers about the importance of the topic and international cooperation in the field: due to the global nature of the ICT supply chain, a national regulatory framework – even by well-resourced countries – can have very limited effect if in isolation. In addition, geopolitics can negatively impact cross-border cooperation – but the increasing geopolitical importance of the supply chain security may as well be an additional incentive.

Interestingly, small countries, once they become aware about the importance of the issue, may be particularly incentivised to set the right regulatory framework in place, and harmonise it with others, in order to become better integrated in the global economy. On the other hand, it is crucial to ensure that those countries that are major producers of digital products (for instance, the IoT devices) are involved in cross-border cooperation.

## 5. International processes

### Multilateral processes

Since the security of digital products is framed in different ways in various countries, as discussed earlier, this topic also cuts across deliberations in a variety of international fora. Of particular relevance are the traditional *security* venues (like UN, OSCE, etc.), *e-commerce* negotiations (in WTO, as well as in G7 and G20), and *standardisation* organisations (international SDOs like ITU, ISO, and IEC).

UN OEWG provides an opportunity to further reduce the gap between the international norms and their operationalisation on national levels. It may build on the UN GGE report of 2021 which laid out certain concrete recommendations on how national frameworks should address issues related to supply chain security, vulnerability treatment, etc. OEWG, however, remains primarily focused on setting norms for responsible behaviour of states, and has limited space for inclusion of the industry and technical and non-governmental communities. Still, there is a value in messaging from the highest levels down to government agencies, which may result in action being taken.

True operationalisation is achieved by international standards. In this field, there are already international regulations on governance of standardisation, accreditation, conformity assessment, and mutual recognition, that minimise fragmentation and burden on enterprises. ITU, ISO, and IEC remain the main space for engagement of states and national authorities, while being open to participation of other stakeholders. The challenge remains in how to better connect their work – and the work of their member states – with other standardisation development venues, like IETF, IEEE, ETSI, and various emerging community, industry, and open standard initiatives which are more agile and closer to the practitioners' demands.

From the economic point of view, OECD's Working Party on Security in the Digital Economy has taken the lead in laying down the groundwork for national policies for digital security of products. OECD recommendations provide main areas and policy options that national policy-makers should look into, as well as integrate in their national systems. OECD recommendations are not binding, but signatories have strong commitment to them. In addition, their work in the field is open to a number of industry representatives, and tends to increase inclusiveness.

WTO may also play an important role in future, with its work on classification and harmonisation of digital products and services, as part of the negotiations on electronic commerce. These negotiations include questions like access to the software source code, and the related security considerations.

### Multistakeholder venues

Number of multistakeholder and industry-driven venues also address securing the supply chain and digital products through principles, recommendations, and good practices, exchange of information, connecting stakeholders and capacity building:

- Geneva Dialogue on Responsible Behaviour in Cyberspace
- Paris Call for Trust and Security in Cyberspace
- Charter of Trust
- Cybersecurity Tech Accord
- World Economic Forum
- The Common Criteria
- UN Internet Governance Forum (and its Best Practices Forum on Cybersecurity)
- Global Forum on Cyber Expertise

### 6. Broader context

The security of digital products is not – and should not be – connected to cybersecurity discussions only. A more secure digital environment enables economic growth and development, and supports human rights and privacy.

National and international processes related to bridging the digital divide, for instance, could be used to incentivise countries to develop policy measures for security of digital products, and ensure transfer of knowledge and experiences from developed countries to developing ones. Connecting a secure digital environment with particular Sustainable Development Goals, for instance, may be one of the approaches. Encouraging development agencies and donors to introduce criteria for the security of digital products to their support programmes may be another.

Inclusion of the economic considerations in the push for regulations, norms or standards is essential to encourage buy-in by national authorities. Human rights and privacy aspects, on the other hand, may serve as a buy-in for many non-government communities, as well as some industries.

### 7. Capacity building

Security threats are the same for all the actors, but different actors may have different risk appetite or tolerance. Training and education are the key for enabling each actor – and each country – to find their own approach to secure the digital environment.

On the one hand, capacity building efforts should increase awareness about the overall context, existing principles and standards, and good (and bad) regulatory and industry practices. Also, capacity building should provide different stakeholders with skills to customise all this to their own needs. It should target a broad range of actors: decision-and policy-makers, regulators and other public authorities, as well as the industry, tech communities, and, even, ranges of customers.

Importantly, capacity building should also develop capacities for these actors to meaningfully participate in and contribute to international dialogue, and understand the broader geopolitical context, as well as the narrower context of technology and innovations. In a way, it should help diplomats and policy-makers understand what’s ‘under the bonnet’ and why vulnerabilities cause such a risk for economy and society, while at the same time it should help CISOs to become ‘diplomats’ and ‘politicians’ of a sort.

## Resources

Number of relevant resources were shared by participants during the event:

1. Security of digital products and services: Reducing vulnerabilities and secure design: Good practices – Geneva Dialogue document from the end of 2020 sets out the definitions related to secure design that have been agreed upon by the partners and highlights some of the best practices that the industry partners are following.
2. Security of digital products and international standards – Messages from the Geneva Dialogue open discussion event, held in May 2021.
3. UN General Assembly 76th Session: Analysis of high-level statements – Diplo's coverage of the 76th debate of the UN General Assembly, illustrating the shift towards digital policy issues in statements delivered.
4. Background Press Call by Senior Administration Officials on Executive Order Charting a New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks – Strong endorsement of Singapore's CLS approach during a press briefing regarding US Executive Order 14208.
5. International Cybersecurity Certification Framework: Pathways to Collaboration and Situational Analysis – WEF briefing paper examines current certification and harmonisation issues, and recommends a sense of collective responsibility which should lead to collective action; an international platform to facilitate cross border recognition of cybersecurity certification.
6. Cybersecurity/Trust – ITU coverage of emerging trends related to cybersecurity and trust.
7. Regulations - DESC – Repository of Dubai's cybersecurity regulations.
8. IoT Device Criteria – NIST's approach to labelling security of IoT devices as part of its assignment under Executive Order 14028. It proposes an initial baseline criteria for consumer IoT device security that will underpin the cybersecurity label. Available for public comments until October 17.
9. Improving the Nation's Cybersecurity – Paragraph 88 of the Executive Order 14028, detailing two labels planned for software and the IoT products.
10. New ITU standards to overcome the security limitations of passwords – ITU standards for a world without passwords, addressing biometric authentication on mobile devices and the use of external authenticators.
11. ETSI EN 303 645 V2.1.1 (2020-06) – The standard describes building security into IoT products from their design.
12. Secure by design – All UK government publications, including Consultation, Code of Practice, Call for Views, and consumer research.
13. Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) v 2.0 – Resource shared as an example of embedding security standards/requirements within safety requirements/regulations in medical devices.

14. Government response to the “Regulatory proposals for consumer Internet of Things (IoT) security” – Results from a UK government’s consultation on regulatory proposals for consumer IoT security.
15. Manufacturer Disclosure Statement for Medical Device Security – MDS$^2$ forms and ‘compliance’ is an industry initiative trying to align and embed cybersecurity into medical devices.
16. Why ITU-assigned numbering ranges are critical to road safety – The article shared as an example of embedding security standards/requirements within safety requirements/regulations.
17. OECD reports on digital security of products and vulnerability treatment – The reports show a significant gap between end-of-life (end of manufacturer’s support) and end-of-use stage, and caution against the emergence of internet of forgotten things.
18. Report on the US CLOUD Act – Report regarding the Cloud Act published by the Swiss Department of Justice explaining that, in order to bring back legal certainty, an Executive Agreement with the US could present a solution for Switzerland.
19. UN GGE and OEWG – Geneva Internet Platform’s coverage of UN GGE and OEWG processes and results.
20. Statement of Intent regarding the security of the Internet of Things by Ministers of Interior, Homeland Security and Public Safety of Australia, Canada, New Zealand, the United Kingdom and the United States – Resource shared as a possible mechanism for cross-border cooperation.
21. Executive Order 14028, Improving the Nation's Cybersecurity – The article details NIST’s responsibilities to enhance cybersecurity under the Executive Order.
22. Consumer IoT Quick Guides and Infographics – The Internet of Things Security Foundation and Oxford information labs infographics, and quick guides on Consumer Internet of things.
23. NIST Risk Management Framework – NIST SP 800-53 Public Comments Overview.
24. NCCoE Learning Series Fireside Chat: Federal Government Perspectives on Managing Supply Chain Cybersecurity Risks to Computing Devices – A fireside chat about supply chain cybersecurity risk.
25. Mapping Security & Privacy in the Internet of Things – This site maps global IoT security and privacy recommendations to the UK’s Code of Practice for Consumer IoT Security, produced by the Department for Digital, Culture, Media & Sport (DCMS).
26. Cybersecurity Labelling Scheme (CLS) – Singapore cybersecurity labelling scheme landing page.
27. Singapore’s Exercise Cyber Star – The coverage of Singapore’s Cyber Star Exercise with complex cyberattack scenarios to strengthen Singapore's readiness.
28. Dubai excellence program – Creating competition between cybersecurity

## Background

The Geneva Dialogue on Responsible Behaviour in Cyberspace, led by the Swiss Federal Department of Foreign Affairs (FDFA), and implemented by DiploFoundation, helps shape a joint vision regarding the security of digital products with leading businesses, and enhances their understanding of and contribution to global policy processes to achieve a trusted, secure, and stable cyberspace. Building on its ground-breaking work, most notably the collection of good industry practices, the Geneva Dialogue endeavours to enhance the feedback loop between corporate efforts and cybersecurity processes that develop norms, regulations, policies, and standards.

As part of its 2021 agenda, Geneva Dialogue will organise three online discussion events, to connect industry practices to processes on norms, regulations, and standardisation on security of digital products:

- ‘Security of digital products and international standards’, May 2021
- ‘Security of digital products and the regulatory environment’, 29 September 2021
- ‘Security of digital products and global norms and principles’ (TBC)

Each online event will consist of several short sessions, and involve – by invitation only – representatives of leading global companies, standardisation organisations, diplomatic missions, international and regional organisations, and national regulators, as well as academic and civil society communities.

## Annex

List of institutions and organisations, participants in the first discussion: 'Security of digital products and the regulatory environment' (29 September 2021)

Representatives of states, institutions and regulators, and regional and multilateral organisations:

- Australia
- Cambodia
- Canada
- Costa Rica
- Finland
- Latvia
- Mongolia
- Netherlands
- Peru
- Singapore
- Slovenia
- Switzerland
- UAE
- UK
- USA
- African Union
- European Union
- OECD
- OSCE

Representatives of the international standardisation organisations and technical community:

- IEC
- IEEE
- IETF
- ISOC
- ITU
- VDE e.V.

Representatives from the industry:

- ABB
- AI Policy Consulting
- AIDirections One Innovation & Artificial Intelligence Research & Consultancies L.L.C
- Amazon Web Services (AWS)

- BI.ZONE
- Copper Horse Ltd
- Ensign InfoSecurity
- Huawei
- Kaspersky
- Liland IT
- Microsoft
- MITRE Corporation
- SICPA
- SwissRe
- TCS
- Tech Mahindra LTD
- UBS AG
- Vega Systems
- Enedis

Representatives of the academia, non-governmental organisations, and other communities:

- Center for Security Studies, ETH Zurich
- Copenhagen Business School
- CREST International
- DiploFoundation
- ETH Zürich
- GEODE
- Queen's University
- THALES
- Kenya ICT Action Network
- Paradigm Initiative
- PNG Digital ICT Cluster Inc.
- Swiss Digital Initiative
- Unifr