GENEVA DIALOGUE ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

Online event

‘Security of digital products and international standards’

28 May 2021

Report and messages

Context

International standards play a significant role in securing the digital environment, including with regard to products. However, the fast-changing environment introduces great challenges. The threat landscape continuously evolves, with increasing sophistication in techniques, tactics, and procedures, including those posed by well-resourced advanced persistent threat (APT) groups. High socio-economic and political impact of cyberattacks demands approaches which transcend the market competition and opt-in compliance. At the same time, the digital supply chain ecosystem is becoming increasingly complex, with a multitude of small and medium enterprises and start-ups, as well as non-tech industries, providing important elements of the supply chain. Products and business practices are being shaped at a much faster pace than standards and the regulatory and normative environment. All this introduces challenges to the development and efficiency of implementation of standards: real-life examples indicate that even those companies which comply with the standards and certifications are not necessarily capable of fending off sophisticated attacks.

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 in digital products.

The first such discussion, ‘Security of digital products and international standards’, took place on 28 May 2021. Representatives of companies, standardisation organisations, and communities, national regulators, government officials, 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 four segments:

1. High-level updates: ‘Standardisation on security of digital products: trends and challenges’

The session hosted high-level representatives of the leading standardisation organisations:

- Gilles Thonet, Director of General Secretary's Office and Deputy to the General Secretary, International Electrotechnical Commission (IEC)
- Chaesub Lee, Director of Telecommunication Standardization Bureau, International Telecommunication Union (ITU)
- Konstantinos Karachalios, Director of Standards Association Managing, Institute of Electrical and Electronics Engineers (IEEE)
- Lars Eggert, Chair, Internet Engineering Task Force (IETF)
- Charles-Pierre Bazin de Caix, Technical Programme Manager, International Organization for Standardization (ISO)

Discussion, moderated by Florian Schütz, Federal Cybersecurity Delegate of Switzerland, provided updates on the work of the leading standard-setting organisations in the field of security of digital products, and explored ways to address main challenges of the fast-changing environment.

2. Focused Discussion: ‘Security of digital products: challenges in the development and implementation of standards’

The session, moderated by Laurent Bernat, Policy analyst at OECD, and co-moderated by Marilia Maciel, Senior researcher at DiploFoundation, allowed for an open discussion on availability of standards in the field, and challenges faced through their development and implementation.

3. Focused Discussion: ‘How to enhance the development and implementation of international standards for the security of digital products’

The session, moderated by Seán Doyle, Lead at the World Economic Forum Centre for Cybersecurity, and co-moderated by Andrijana Gavrilovic, Researcher at DiploFoundation, allowed for an open discussion on ways of addressing the challenges identified in the previous session, and focused at the fora in which this dialogue could continue

4. Takeaways and closing

The closing session with Jonas Grätz, Political Affairs Officer at the Federal Department of Foreign Affairs of Switzerland, and Jovan Kurbalija, Director of DiploFoundation and Head of the Geneva Internet Platform, provided key takeaways and possible further steps for this discussion.

Key messages

Key messages were prepared based on the discussions and the exchange among professionals from standardisation organisations, regulators, diplomats, industry experts, and other event participants. 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

Part I: Challenges in the development and implementation of standards

1. **Fast-changing environment**
   - The pace of technological development is ever increasing. On one hand, the existing products are constantly improved: they receive updates and fixes (which are commonly not considered as a different product), and are every so often replaced with new product versions on the market. On the other hand, new and complex digital technologies are emerging: internet of things (IoT) and smart environments, machine learning and artificial intelligence, 5G/6G and advanced connectivity, quantum computing and communications, virtual, augmented and mixed reality, brain to computer interfaces, etc.
   - At the same time, standardisation development organisations (SDO) react to specific challenges and needs presented by various communities. Such a process requires involvement of numerous actors (and increasing number and profiles of those). Most of the standards are being agreed on by (rough) consensus, which is time consuming process as it relies on dialogue, understanding, and trust.
   - In the meantime, the threat landscape advances as well. Threat actors are enhancing their resources, capabilities, and tools, and exploring new approaches to exploit vulnerabilities in the weakest links of the supply chain. The traditional 'check-lists' approach to security seems to be obsolete.

2. **Convergence of technologies**
   - The borders between different technologies are becoming blurry. For example, the widely used IT technologies were typically different from specific industrial and operational technologies (OT). Today, OT systems are becoming 'smart' and connected, while various IoT and other 'off the shelf' products (which were not developed with industrial use in mind) find their application in industrial environments.
   - Due to the different nature of security challenges of the IT and OT systems, the standardisation efforts which were addressing them were separate. With the convergence of technologies, those separate streams of standardisation processes need to be better connected and synchronised. In addition, the integration of different types of products brings about new security challenges that were previously not addressed by either of the streams.

3. **Supply chain complexity and new actors around the table**
   - Supply chain is getting increasingly complex. A single digital product or solution may include hundreds of components from various vendors around the world: from software libraries to hardware components and IoT devices. Vulnerability in each component of the supply chain, regardless of how minor or uncritical it may seem, may be exploited for a sophisticated cyberattack resulting in global consequences. Suppliers of products are often unaware of what their product fully consists of.
   - This brings into play new types of vendors and producers that may have critical roles in the supply chain security, such as the open-source community, start-ups and micro, small, and medium enterprises (MSME). Such actors have, traditionally, not been considered as 'critical', and their level of compliance to certain standards was typically not an issue.
   - At the same time, 'traditional' SDO still lacks specific standards related to the security of certain supply chain components. The development community – such as the open-source community – started self-organising and shaping its own proposals for standards, which should then be put forward at major SDO with the idea of becoming international standards.

4. **Cybersecurity as a political concern**
   - As cybersecurity climbs up the ladder of political importance, governments are focusing on devising national policy responses. Regulatory authorities are increasing their work on various schemes in order to enhance the security of digital products – from both the vendor's and the consumer's side.
   - There is a risk that emerging regulatory approaches may outpace the emergence of corresponding standards, or anchor themselves to available standards (not agreed on as international standards) of their preference, potentially leading to a fragmented regulatory environment. Without the firm cooperation between standard-setting communities and regulators and governments around the world, a fragmented regulatory environment may emerge, introducing obstacles for businesses and economic cooperation.
   - At the same time, many states invest in the development of new technologies as part of their strategic interests. States are increasingly aware of the political and economic importance of standards, in particular with regards to cybersecurity. While, on a positive side, this may lead to greater investment in synchronised international standards and their adoption on national levels, it may also introduce risks of greater politicisation of standard-setting processes and organisations, and framing cybersecurity standards as an issue of national security concern.

5. **Slow implementation and limited effectiveness of standards**
   - The fast-changing threat landscape and increasingly complex supply chain indicate that compliance with standards ('check-list') is no longer sufficient, which is evident from recent supply chain attacks. A risk-based approach and the assessment of real effects of security measures is needed.
   - A focus on normative security requirements favours organisations which can afford them. Many actors, and particularly MSME, do not have sufficient awareness, incentives, resources, and knowledge needed to follow and implement security standards.

- Vendors are not the only ones that produce digital products: an increasing number of local authorities and municipalities, non-government organisations, and media, for instance, are developing gadgets, applications or services on their own. Their awareness of security concerns and applicable standards is a limited one, as is that of various donor communities that support them.

6. **Industry challenges**

- Corporate budgets for compliance with standards are less likely to expand than to shrink. This could further limit the innovative approaches to product security (beyond mere compliance).
- Conformity with security standards is not among the companies' top priorities, as they mostly focus on selling their products as fast and widely as possible. Developers are typically asked to focus on functionality rather than on security. Companies are not ready for a trade-off on 'speed to market' versus conformity. In most cases, it is not illegal to use insecure products, while it also saves the costs.
- Fast-changing standards' environment makes it hard for industries to switch (or extend) from one set of requirements to another. Unsynchronised regulatory environments make this even harder, as global companies need to follow different requirements across jurisdictions.
- Due to the increasing complexity of the supply chain, vendors often do not fully understand their products: what third-party components and dependencies are within them, and how the vulnerabilities of those could impact their own product and clients.

Part II: Ways to enhance the development and implementation of international standards

A. **Standards development**

Overall approach to standards may be re-visited in order to better address the challenges. This may refer to:

- Focusing standards on outcomes, rather than on controls: looking at risk-based or threat-based standards, to reflect the ever-changing threat environment.
- Moving away from the reactive work on documenting the common practices, towards better proactive following of needs and risks (e.g. some ITU-T Focus Groups address the fast evolving needs – like FG-QIT4N on quantum IT for networks).
- Incubating innovative ideas through cooperation with various actors and professionals (e.g. IEEE Standards Association has the Industry Connections program which helps incubate new standards and related products).
- Changing the mindset of the communities beyond compliance: to better understand the importance of security of digital products for the global cybersecurity and stability, and perceive it rather as a component of ethical industry behaviour than just compliance.
- Analysing the multiple dimensions of standards: technology, business, and economy, as well as (geo)politics.

- Taking into consideration the 'implementability' of standards and possibilities for conformity assessment, for example, through conformity assessment systems within SDOs (e.g. IECEE, the IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components), consulting with actors that would play this role, and considering the risk tolerance and risk appetite of the various actors that should apply the desired standard.
- Considering standards as a type of product, and finding the 'buy-ins' for industries and others to embrace them.
- Putting more emphasis on standards related to processes (such as the secure development lifecycle and the organisational practices) and particularly people (advancement of multidisciplinary skills and certification of labour), rather than just on the products.

Agile processes and procedures to develop standards should include, among other:

- Continuous adaptation of standards, in accordance with the evolution of the threat landscape: assessment, management, and mitigation of risks.
- Understanding of the needs of a greater diversity of stakeholders, and development of standards in an inclusive and bottom-up manner (e.g. IEC Standards Evaluation Groups (SEGs), such as on biodigital convergence, are pre-standardisation groups fully open for anyone to contribute to building standardisation roadmap)
- In that regard, involvement of greater diversity of actors in processes, such as national institutions (standardisation, regulators, decision-makers), conformity assessment bodies, open-source communities and MSMEs, researchers, and other SDO (including open-standards communities), and finding ways to incentivise those actors in participating in the process (e.g. IETF work is inclusive, open source and without fees, based on rough consensus).
- Using modern IT tools to allow for more effective collaboration (e.g. embrace virtual meetings for inclusiveness and consultations) and allowing organisations to embrace them in an easier and better automated way (e.g. standards readable, interpretable, and updatable by machines themselves).
- Elaborating on review mechanisms to address challenges with, as well as on flaws in standards, including possible security implications of standards themselves (e.g. 3GPP is a good example of such mechanism).

New formats of standards might require consideration along with the 'traditional' ones:

- Packaging standards could provide 'a la carte' customisable set of requirements (by various SDOs) for a particular product (e.g. a customised package of standards for an e-bike, instead of requiring it to follow dozens of more generalised standards).
- 'Lite standards' may focus on the minimal level of security for digital products which are not deployed within critical systems, as baby steps stimulating further certification.
- Baseline requirements or recommendations can present the minimum of internationally agreed requirements (e.g. Charter of Trust baseline requirements on security-by-default, or the NIST IoT baseline requirements).
- 'Greenfield graphs' specifications can be developed for specific areas, to help assessing the quality of systems (e.g. IEEE greenfield graphs for AI systems).

- Commonly agreed on principles could address the 'unknown unknowns' and serve as a common ground for cooperation across SDOs; some examples include securing the weakest link, granting least privilege, authenticating requests, controlling access, making security usable, securing defaults, trusted components, and promoting privacy (e.g. IEEE foundational security principles).

Consistency and synchronisation of standards is essential. Opportunities to address this include:

- Enhancing cooperation across SDOs and consortia – including cooperation with open standards and open-source communities (e.g. OWASP) – for mutual recognition, adoption of specifications, and creating a holistic approach in addressing critical and converging technologies (e.g. boards of the ITU, ISO, and IEC meet for coordination and resources; others may be involved as well),
- Synchronising standards across industries and countries, through interconnecting national standardisation organisations and regulators, as well as with industries and across international SDOs.
- Addressing converging technologies through connecting standards within and among SDOs (e.g. connecting ISO 27000 series on IT security with IEC 62443 series on OT security), but also through bringing the IT and OT communities (SDOs, industries, regulators, researchers) together and bridging the gaps between their professional cultures and mindsets.
- Developing 'missing' standards, such as those for secure software development.

B. **Implementation and efficiency of standards**

Access to standards by a wider community should be enhanced through:

- Promoting open standards.
- Reducing or waiving the fees for access to standards for certain actors or industries (that have limited resources, but whose products might become critical for the supply chain).
- Investing in awareness and capacity building of various industries and actors, in particular those with very limited resources.

Compliance and conformity assessment should be improved. Some of the possible mechanisms for achieving this include:

- The development of standards for evaluators and auditors, and building their capacities and competences.
- A risk-based approach, through assessing the risks from certain industries/products and, based on that, considering multiple levels of requirements (e.g. the Singapore labelling scheme considers multiple levels: from baseline requirements to resilience to common attack) – with flexibility to change the requirements depending on the evolution of the threat environment.
- In addition, a customisable approach to conformity assessment (e.g. self-declaration, third-party evaluation, etc.) and conformity evidence, to gradually push vendors towards greater security levels.
- Separating best efforts from negligence (e.g. 'buffer overflow') and developing methodologies to assess this.

- Continuous attestation: since products regularly get updated or upgraded, it is necessary to certify not only the original product, but its entire life-cycle (including patches and new versions), as well as the organisational processes around it.
- Developing assurance cases (AC), as a means to capture and exchange vendor's claims about the security of a product or a process, and the evidence to support those claims (building up on community standards for capturing AC, like Goal Structuring Notation (GSN), Claims-Arguments-Evidence (CAE), or Structured Assurance Case Metamodel (SACM), as well as on the related standards like ISO/IEC 15026 on system and software assurance).

It is also necessary to move beyond compliance by:

- Testing weaknesses in products and systems, and assessing the effectiveness of cybersecurity measures, rather than simply checking formal compliance with standards.
- Boosting the incentives for greater product security, through market advantages, greater demand for secure products (e.g. through certification and labelling schemes), etc.
- Developing other tools apart from standards, such as requirements and expectations, documented good practices, etc.
- Nurturing the engagement of broader communities in incentivising and assisting industries with implementations of security measures (e.g. researchers with vulnerability disclosure).

National regulatory frameworks are of great importance:

- Increasing concern for cybersecurity on national levels should be harnessed for a greater uptake of standards.
- In creating a risk-based approach, regulators should also take into consideration the specific threat environment of the country or region.
- A demand for more secure products can be boosted by national certification and labelling schemes (e.g. in Singapore, Finland, European Union, Dubai, etc.), which would in turn push industries to embrace standards and good practices.
- Regulators might also need to consider liability of the producers, in view of certain incidents that were enabled through insecure products.
- To support the global economy and avoid fragmentation of the market, regulators should align their instruments (e.g. certification schemes) with common international standards.
- In this regard, regulators should be more involved with the work of the SDOs, in order to be able to better understand the diversity and roles of specific standards, and receive guidance on how to select the appropriate standards and combine them.
- Similarly, regulators should work more closely with the national standard organisations that are members of some SDOs, with conformity assessment bodies to verify the implementation of standards, as well as with their decision makers in order to raise awareness about the importance of international standards for 'protecting yourself by protecting everyone' concept.

- At the same time, regulators should closely collaborate with the private sector, to identify feasible solutions and address specific challenges (e.g. time-to-market considerations, costs of compliance, risk tolerance, and risk appetite).
- Finally, there is a need for greater cooperation among the regulators and decision makers across jurisdictions, to synchronise their efforts to reduce trade barriers and avoid different certification criteria across the world.

Industry, of course, plays the key role in enhancing security of its products:

- One of the main challenges which needs addressing is the initiation of a cultural and a mindset shift among the industry leaders, to embrace security as the integral and pivotal component of products and processes.
- In this regard, external security events and incidents can be showcased to raise awareness of the risks; competition also plays its role, particularly when a demand for a secure product is growing (e.g. the case of Zoom security measures).
- In responding to this, producers have to manage both the requirements for standards and the expectations for security. And, they must become aware of the risks which stem from the use of their products in different environments (e.g. in critical infrastructures).
- Certain existing standards are of a clear practical importance for industries (e.g. standards on information exchange, such as ITU/ISO/IEC X1215 for operators to share threat information); enhancing the promotion of such standards within the relevant industries could help raise awareness about the importance of standards themselves and of participation in standards development processes.
- Industries need, to an increasing extent, assistance in dealing with real security challenges, rather than simple compliance.
- Certain pre-standardisation efforts and requirements are of special practical use (e.g. Bill of materials (BOM) as a list of 'ingredients' for each product, and dependencies among products within a supply chain).
- Businesses should provide peer incentives as well as clear security requirements to their partners and suppliers, especially those with limited awareness and resources.
- Capacity building support for companies should transcend compliance and standards, and move towards understanding a broader regulatory and political environment – related both to threats and cooperation mechanisms (from cooperation on standards to global norms and principles).

Part III: Next steps

There is an explicit need for greater cooperation in synchronising different national, regional, and global industry practices, standards, regulations, norms, and principles related to the security of digital products.

A dialogue on such issues would need to involve, among others:

- SDOs
- Businesses/industry (including SMEs and start-ups)
- National standardisation organisations
- National regulatory authorities

- National decision makers
- Conformity assessment bodies/certification authorities
- Broader communities (open source, researchers, etc.)

Suggestions for the follow-up activities include:

- A continuation of the Geneva Dialogue discussions among the variety of actors, focusing on business practices, standards, regulations, norms, and principles.
- A 'Geneva Cyber-Summit for SDOs', with appointed representatives of ISO, IEC, ITU, IEEE, IETF, and other international SDOs and standard-setting communities, in order to exchange best practices and synchronise their work.
- Bilateral or plurilateral dialogues among the leading national regulatory authorities, for synchronisation and mutual recognition of efforts. The establishment of an international dialogue can later follow.
- On a longer term, establishing a "cyber-Bretton Woods" type of a summit to set certain rules for cybersecurity relations, led by the international SDOs (e.g. IEEE, ISO/IEC) and with participation of regulators and others.

Since this event, as well as the significant part of the global dialogue on cybersecurity standards and norms being linked to Geneva, a new adage emerged: "All cyber-roads lead to Geneva". Geneva Dialogue, along with ISO, IEC, and ITU, and with support of the Geneva Internet Platform, WEF, OECD, and other partners, could contribute significantly to the dialogue among diverse actors.

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', 2021 (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 international standards' (28 May 2021)

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

- PRIDA, Africa Union Commission
- Department of Home Affairs, Australia
- DG CONNECT, EU Commission
- Dubai Electronic Security Center, UAE
- BSI, Germany
- Ministry of Foreign Affairs, Netherlands
- Ministry of Economic Affairs and Climate Policy, Netherlands
- Organisation for Economic Co-operation and Development (OECD)
- Cybersecurity Agency of Singapore
- Federal Department for Foreign Affairs, Switzerland
- State Secretariat for Economic Affairs SECO, Switzerland
- NTIA, US Department of Commerce

Representatives of international standardisation organisations:

- International Electrotechnical Commission (IEC)
- International Organization for Standardization (ISO)
- International Telecommunication Union (ITU)
- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)

Representatives of the diplomatic community in Geneva:

- Permanent Mission of Afghanistan
- Permanent Mission of Canada
- Permanent Mission of Dominican Republic
- Permanent Mission of Estonia
- Permanent Mission of Finland
- Permanent Mission of Mongolia
- Permanent Mission of Slovenia

Representatives from the industry:

- BI.ZONE
- Cisco
- Ensign InfoSecurity
- Huawei
- Kaspersky
- Microsoft
- MITRE Corporation
- SICPA
- Siemens

- SwissRe
- Tata Consultancy Services (TCS)
- VDE/DKE
- Wipro Limited
- WiseKey

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

- China Academy of Information and Communications Technology (CAICT)
- Cyber Peace Initiative
- Cyber Risk Institute
- DiploFoundation
- ETH Zürich, Center for Security Studies
- Geneva Internet Platform
- ICT4Peace Foundation
- Konrad Adenauer Stiftung
- University College London
- World Economic Forum

Contact

Vladimir Radunovic, DiploFoundation, vladar@diplomacy.edu
Jonas Grätz, FDFA, jonas.graetz-hoffmann@eda.admin.ch

For more about Geneva Dialogue, visit: https://genevadialogue.ch, or contact: genevadialogue@diplomacy.edu

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

DiPLO
www.diplomacy.edu