WORLD TRADE ORGANIZATION

G/TBT/GEN/357

20 July 2023

(23-4958)

Committee on Technical Barriers to Trade

THEMATIC SESSION ON REGULATORY COOPERATION BETWEEN MEMBERS ON CYBERSECURITY

20 JUNE 2023, 15:00-18:00

Moderator's Report[1]

At the Ninth Triennial Review, Members agreed to continue to hold thematic sessions in conjunction with the Committee's regular meetings from 2022 to 2024, with a view to further deepening the Committee's exchange of experiences on specific topics. On this basis, the Committee agreed to hold a thematic session on regulatory cooperation on cybersecurity.[2] The thematic session provided an opportunity to explore the role of technical regulations, standards and conformity assessment procedures in contributing to Members' policies to address cybersecurity threats. Members discussed existing approaches in managing cybersecurity risks and the opportunities for regulatory cooperation. Information about the speakers, presentations, and related materials are available on the WTO website.[3]

1 INTRODUCTORY REMARKS BY THE MODERATOR

1.1. The thematic session was timely, particularly against the backdrop of Members' growing discussion of the policies and regulations on cybersecurity at the TBT Committee.

1.2. To illustrate, first, Members have notified around 80 (as of 31 May 2023) cybersecurity-related measures to the TBT Committee. This was clearly a new trend because the vast majority of these (over 60%) were only notified since 2020. Such notifications dealt with a wide range of products and situations, for example: the cybersecurity of Internet of Things (IoTs), 5G technology, telecommunication, vehicles and radio equipment and software-enabled and network-connected goods. Around half of these measures indicated that they have been proposed or adopted for the protection of national security interests.

1.3. Second, in recent years, WTO Members have increasingly used the TBT Committee to raise and discuss specific trade concerns (STCs) with various cybersecurity-related measures. These measures subject to these STCs regulate, for instance: ITC products and network equipment, vehicles, civil aviation, banking, and insurance. To date, Members have raised at least 26 such STCs, the majority of which (60%) during the last six years (2017- May 2023). These discussions are important given the nature of the topic as well as the quantitative value of the STC involved. According to estimates by the WTO Secretariat, the average imports per STC related to cybersecurity amounts to almost USD 160 billion. Indeed, cybersecurity-related measures are the most significant type of STCs by value, as compared to the rest of STCs relating to the other "topics".

2 DISCUSSION

2.1 Guiding questions

- What are the challenges and opportunities of trade and regulation of cybersecurity?
- How do the disciplines and principles under the WTO TBT Agreement contribute to effective trade policies to ensure cybersecurity? What role can the TBT Committee play?

[1] Mr Wei Guo Tang (Singapore). This Report is provided on the Moderator's own responsibility.
[2] G/TBT/46, para. 2.11.
[3] WTO | Thematic session on Regulatory Cooperation between Members on Cybersecurity.

- What best practices should guide the development and implementation of regulations in this area? What role can international standards play in this regard?

3 INTERVENTIONS

3.1. **Mr Mike Mullane** (IEC)[4] presented the IEC's work on cybersecurity standards, focusing on the organization's ecosystem approach to standard-making in this area. The IEC develops both horizontal cybersecurity standards that address informational and operation security and vertical sector-specific standards (e.g. IEC 63154 or ISO/IEC 29128-1). Mr Mullane also discussed some of the key benefits of using standards and conformity assessments in the area of cybersecurity, such as building confidence and trust with trading partners, ensuring consistency through harmonization and increasing market access and global recognition. He further elaborated on the risk-based approach of IEC standards, which encourage businesses to rank their assets by security level required. Mr Mullane concluded by highlighting the importance of global collaboration to tackle cybersecurity threats and encouraged members to adopt the IEC's common framework of standards.

3.2. **Ms. Nandini Jolly** (Canada)[5] explained that in the aftermath of the covid-19 pandemic and in the current geopolitical climate data centric security (as opposed to solely network security) is becoming increasing important. She introduced CryptoMill's zero trust approach to cybersecurity, which aims to shift towards data centric security and highlighted the importance of recognizing risks as existing both inside and outside a network.

3.3. CryptoMill services specialise in resolving issues associated with external hacks, internal data leaks, ransomware, supply chain vulnerabilities, misdirected emails, lingering data and stolen devices. Ms. Jolly also presented the company's Circles of Trust Software Suite, a security platform providing businesses, military and governments control over the access to all sensitive data and its use, which for example also for data shared with business partners to remain protected. She concluded by raising concern on the cybersecurity risks associated with the increasing popularity of hybrid work Ms. Jolly reiterated the important need for collaboration and cooperation, including in the area of standards, to identify and solve those risks. Collaboration can help improve information sharing to speed up the technology developments needed to address these threats.

3.4. **Mr Jonathan McHale's** (United States)[6] presentation focused on the need for cooperation and global solutions to address cybersecurity threats. He explained that national measures targeting the digital world, such as national encryption or Wi-Fi security requirements clearly distort trade, with no obvious benefits, and measures such as data localization can sometimes undermine global cybersecurity by limiting global visibility into existing threats. In his view, a global standardization response is needed to address cybersecurity threats, in a digital world, that by design is also global. Mr McHale stressed that cooperation is needed to achieve a global consensus on what the most significant cybersecurity threats are, in order to efficiently use resources to tackle these. He concluded by reminding the audience of the key factors to consider when cybersecurity developing standards, such as the compliance requirements of such standard, the stakeholder engagement in its development process and its trade impact.

3.5. **Ms Adv Jacqueline Fick** (South Africa)[7] stressed the importance of international cooperation and harmonisation in creating cyber-related legislation, with the aim of increasing cybersecurity posture and data privacy. Adv Fick explained that cybersecurity and cybercrime are interlinked issues which must be addressed together. To address these connected issues, she suggested a cross-border, collaborative approach to address the borderless nature of cybercrime: mechanisms that are efficient and effective to deal with issues that happen at a great speed. Cyber-related legislation is crucial because it underpins effective e-commerce, increases trusts between countries, enhances incident response, as well as the ability to where necessary, bring cybercriminals to book. Therefore, Adv Fick underscored that harmonisation, international cooperation and standardisation are needed to not only create useful international instruments, but to also enhance certainty regarding globally accepted cybersecurity practices, measures to address cybercrime and to facilitate the sharing of electronic evidence between countries that are admissible in a court of law. There is no need to "re-invent the wheel". None of these efforts should be viewed as an attempt to interfere with a countries'

[4] Advocacy Officer, IEC.

[5] CEO, Crypto Mill Cybersecurity Solutions, Canada.

[6] Vice President of Digital Trade, Computer & Communications Industry Association, United States.

[7] CEO, VizStrat Solutions, South Africa.

sovereignty, but more in enhancing a global cybersecure environment. Adv Fick outlined the South African government's priority to address cybersecurity and their legislative approach. She also called for increased training and awareness on cybersecurity and mutual legal assistance and information sharing.

3.6. **Mr Jiefu Gan's** (China)[8] presentation advocated for the need for more inclusive multilateral cooperation on cybersecurity standardization and conformity assessments. Within the space, he listed some of the opportunities and challenges. According to Mr Gan, there are opportunities in the areas of digital economy, data and digital products as well as cybersecurity and data security. Notable challenges include global digital governance deficit and subsequently, a risk division and fragmentation of digital governance.

3.7. Mr Gan proposed several suggestions namely: keeping markets open and free from discrimination, more global unity and cooperation by creating interoperable and common rules, balance between development and security, commitment to fairness and justice and more inclusive cooperation on cybersecurity standards and conformity assessments. Finally, he provided examples of practices in China. Several measures have been adopted including use of conformity assessment procedures as one of the technical support means for cybersecurity management and legislation implemented to promote certification and standards.

3.8. **Ms Huirong Tian** (China)[9] presented on the standardization activities on cybersecurity and data protection in ICT areas in China. She outlined the 4 main types of standards in these areas: (i) national, (ii) industry, (iii)association and (iv) enterprise and their different scopes. There are several Standardization Technical Committee (TCs) for each area. For example, national security standard is mainly organised under TC260. Specifically, industry security standard is organised under China Communication Standardization Association (CCSA), their main security TC is TC8 – a network and data security technical committee. The security work under CCSA includes network security standards, data security standards emerging technology security standards and integrated application security standards. Also important to the CCSA's work is international cooperation and international standards development organisations such as cooperating with IETF, OMA and partnerships with GSC and 3GPP etc.

3.9. **Mrs Amy Mahn** (United States)[10] presented her organisation and its long-established role in cybersecurity since NIST's development of s Data Encryption Standard in the 1970s. She also introduced NIST's Cybersecurity Framework (CSF), which helps organizations reduce their cybersecurity risks and has, in addition to the US, already been adopted by many governments around the world, including Uruguay, Japan, and Italy to name a few. The CSF is guided by many perspectives, from private sector to academia and public sector, and is currently being reviewed based on stakeholder feedback. Mrs Mahn also reiterated points previously raised by speakers on the key role widely accepted standards can play in creating competitive and safe markets and facilitating international trade.

3.10. **Mr Hideyasu Tamura** (Japan)[11] began by raising concerns over the patterns of cybersecurity-measures, that could be trade-restrictive. Those include, for example, requirement for utilizing domestically produced components or software for critical infrastructures, based on security reasons. He reminded the audience of the importance of developing cybersecurity measures in line with the TBT Agreement and in the least trade restrictive way possible. As other speakers, Mr Tamura emphasized the need for a cooperative approach to tackling cybersecurity and notably highlighted the Comprehensive and Progressive Agreement for Trans-Pacific Partnership's (CPTPP) ambitious approach to standard-making. He concluded by addressing the need for cybersecurity labelling schemes, including the harmonization or interoperability amongst them.

3.11. **Mr Mohamad Endhy Aziz** (Indonesia)[12] shared the cybersecurity developments of Southeast Asia over the recent years, highlighting the growing importance of the digital economy to the region. The digital landscape in Indonesia is concentrated in e-commerce and digital services, sectors which

[8] Department Vice Director, China Cybersecurity Review Technology and Certification Centre, China.

[9] Chief Engineer of Security Research Institute, China Academy of Information and Communications Technology (CAICT), China.

[10] International Policy Specialist, National Institute of Standards (NIST), United States.

[11] Senior Director for International Trade Policy Bureau, Ministry of Economy, Trade and Industry (METI), Japan.

[12] Senior Cybersecurity Specialist, The National Cyber and Encryption Agency, Indonesia.

are expected to contribute to at least 14% of the economy's GDP by 2027. However, Mr Endhy Aziz also warned about Indonesia's increased exposure to cyber threats, with a seven-fold increase in cyber-attacks in the past four years. Increasing international cooperation in matters of cybersecurity is, therefore, particularly important to Indonesia, and other ASEAN partners. According to Mr Endhy Aziz, the trade community can take greater steps to increase cooperation on cybersecurity, notably by developing a shared understanding of cyber threats and their scope and agreeing to adopt a risk-based approach to cybersecurity. He concluded by reminding the audience of the importance of also ensuring compliance with common cybersecurity standards while continuing to develop these in the least trade restrictive way possible.

3.12. **Ms Veena Dholiwar** (United Kingdom)[13] provided an overview of the United Kingdom's product security regime which forms part of the government's national cybersecurity strategy. This strategy was motivated by their commitment to protect the interests of and prevent harm to citizens. Key features of the regime include the Product Security and Telecommunications Infrastructure Act 2022. With this Act, the UK's security regime would be the first in the world to require minimum cyber security requirements before consumer IoT or 'smart' products can be sold to UK consumers.[14]

3.13. Ms Dholiwar also summarised the UK's work in developing a voluntary code of practice, international standards, and the path to legislation. She emphasised the collaborative exercise which included stakeholder engagement, public consultations and calls for view as well as research with industry and consumers. She highlights that the regime aligns with TBT transparency obligations, openness, and collaboration. Finally, she highlighted the UK's commitment to international collaboration and sharing their experience with other Member countries.

3.14. **Mr Fabio Polverino** (European Union)[15] **and Mr Luis Miguel Vega Fidalgo** (European Union)[16] presented on the valuable role of cybersecurity regulations for trade. To illustrate the importance of regulation, they detailed the high costs associated with cyber incidents. One clear example was from Germany, where in 2020 the aggregate cost of security incidents affecting businesses amounted to EUR 220 billion. To address the cybersecurity of products, the EU started first addressing wireless devices with the Delegated Act of the Radio Equipment Directive (RED DA) and, with the proposed Cyber Resilience Act (CRA), is now evolving to cover all products with digital elements and throughout their lifecycle. This layered legal approach has allowed to reassess, identify and rectify any gaps found in past legislation.

3.15. The presenters highlighted existing and future regulations, namely: (i) the Delegated Act of the Radio Equipment Directive (RED DA) and (ii) the Cyber Resilience Act (CRA). The RED DA introduced in 2022 is a legislation which focuses on cybersecurity requirements for wireless devices. It addresses a gap in previous product legislation and for the first time imposes obligations on manufacturers of products in terms of cybersecurity. The CRA, proposed in September 2022 and subject to final adoption, builds on existing legislation including the RED DA and fills a legislative gap by introducing mandatory cybersecurity requirements for all products with digital elements, including hardware and software products. The main objective of the CRA is to ensure that manufacturers ensure adequate cybersecurity of products with digital elements made available on the EU market, from the design and development phase and throughout the entire product life cycle. It also seeks to ensure a coherent cybersecurity framework by setting horizontal cybersecurity requirements and it will foster consumer trust by enhancing transparency of security properties. Both the RED DA and the CRA will be implemented via product and/or process standards, building on existing European and international standards. This demonstrates the role and benefits of standards to provide legal certainty, reduce cost compliance costs and avoid barriers to trade amongst other benefits.

4 DISCUSSION

4.1. The discussion featured an open dialogue between the private sector, regulatory representatives, and delegates on their perspectives on and approaches of the topic of cybersecurity.

[13] Head of Enforcement & Evidence, IoT Product Security, DSIT, United Kingdom.

[14] The regime mandates 3 security requirements that manufacturers must comply with before selling to UK consumers.

[15] Policy Officer, Cybersecurity and Digital Privacy Policy Unit, Directorate-General for Communications Networks, Content and Technology (DG CONNECT), European Commission.

[16] Policy Officer, Machinery & Equipment Unit, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW), European Commission.

Participants from the private sector unanimously highlighted the importance for regulatory authorities to promote interoperability, openness to stakeholders consultations, and technical discussions in developing cybersecurity standards and regulations. The participants also expressed their support for the practical measures and approaches offered by the regulators featured on the panel.

4.2. The panel was asked to consider if the robustness of the cybersecurity standards is dependent on the country of origin of the producers or suppliers of digital products. In response, various panellists alluded to existing international standards which would ultimately be country-agnostic.

4.3. There was also wider discussion on the participation of external stakeholders, including businesses, in ongoing domestic and regional collaboration on cybersecurity. In light of the numerous legislation and measures shared during the presentations, WTO members in question were requested to officially notify all new and proposed regulations, standards and conformity assessment procedures as required under the TBT Agreement.

5 COMMENTS BY THE MODERATOR

5.1. It was a very enriching session with inputs from 12 speakers. The key take-aways from the Thematic Session on Regulatory Cooperation between Members on Cybersecurity are as follows:

- Regulatory measures are increasingly used in Members' efforts to tackle cybersecurity. Some speakers warned about such regulations sometimes having the opposite effect of undermining global cybersecurity efforts if taken unilaterally or at the national level. Speakers also raised concerns over the possible trade barriers arising from national cybersecurity measures. In this regard, several speakers highlighted the need to develop a common understanding of existing and future cybersecurity risks, which would also allow to address cybersecurity challenges more efficiently.

- As seen today, efforts to develop ambitious, fair and inclusive international standards in the realm of cybersecurity are well underway. All speakers shared a common understanding that international standards are key to counter cybersecurity threats. Many (if not all) alluded to international initiatives, including the work by standard-making agencies such as IEC and ISO.

- Most speakers (from both industry and government) underscored the need for the government and the private sector to work in a more coordinated and collaborative manner with standards-making bodies. This is essential to address the rising regulatory fragmentation and divergence in addressing cybersecurity concerns and digital governance. This collaboration is also important to address growing cybercrime and cyber incidents. Relatedly, speakers noted that regulators should engage with stakeholders in drafting and enacting cybersecurity measures. This extends across industries and to consumers within the market.

- Developed and developing 'Members shared their experiences in designing, adopting and implementing regulatory measures and standards on cybersecurity in the interest of protecting their citizens. We also heard from international standards-setting bodies, and their ecosystem approach to cybersecurity standard-making, focusing on both horizontal standards that address informational and operation security and vertical sector-specific standards.

- From the private sector, we heard examples from cybersecurity businesses that is in the market of addressing a range of cybersecurity threats. We also heard of common cybersecurity-related regulatory challenges faced by SMEs such as the risk of being priced out of a market when regulations become too stringent and fragmented.

5.2. All in all, the discussions were rich and insightful. The moderator would like to express his appreciation for the thought-provoking inputs from our speakers. He expressed hopes that the TBT Committee will also continue to build on the thematic discussions on regulatory cooperation on cybersecurity.

____