|  |  |
| --- | --- |
|  | **Addendum 6 to Document EG-ITRs-1/2** |
| **7 September 2023** |
| **English only** |
|  |  |
| Contribution from HILL | |
| ART. 6: SECURITY AND ROBUSTNESS OF NETWORKS | |
| **Purpose**  Discussion  **Action required**  The document is submitted to EG-ITRs **for discussion**.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Reference**  [Council Resolution 1379, revised 2023](https://www.itu.int/md/S23-CL-C-0121/en) | |

1. The work of the current ITR-EG is specified in its Terms of Reference[[1]](#footnote-1):

*2 Taking into consideration the work of the previous two Expert Groups, the review may consider, among others:*

*a) new trends in telecommunications/ICT and emerging issues in international telecommunications/ICT environment which may impact the ITRs,*

*b) empirical data on the current use of the ITRs by operating agencies and/or administrations and the proportion of global telecommunication services which now rely on the ITRs, and*

*c) the relevance of the ITRs which “consist of high-level guiding principles” in the current telecommunication/ICT environment.*

2. This contribution focuses on art. 6 of the 2012 ITRs, Security and robustness of networks, which states:

*6.1 Member States shall individually and collectively endeavor to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.*

**Discussion of Article 6**

3. Criticism of this provision has been addressed in academic writings[[2]](#footnote-2), [[3]](#footnote-3).

4. Starting in 2017, several Member States, in particular developed countries, proposed that provisions regarding cybersecurity should be included in free trade agreements, including those agreed in the World Trade Organization (WTO).

5. Indeed, Security experts have long recognized that the lack of information and communication technology (ICT) security creates a negative externality.[[4]](#footnote-4) For example, if an electronic commerce service is hacked and credit card information is disclosed, the users of the service will have to change their credit cards. This is a cost both for the end user and the credit card company. However, that cost is not visible to the e-commerce service. Consequently, the service does not have an incentive to invest in greater security measures. Furthermore, users do not have the information or the technical expertise required to determine whether any particular product or service has adequate security. That is, there is an asymmetry of information in which the supplier knows more than the customer.[[5]](#footnote-5)

6. Such market failures can only be corrected by regulatory action, specifically, by imposing liability on suppliers of insecure devices and/or mandating minimum security standards. This is the case for airplanes, automobiles, electrical appliances, pharmaceuticals, etc. Why should it not be the case for ICTs?[[6]](#footnote-6)

7. As stated in 2017 by the Microsoft president[[7]](#footnote-7):

The time has come to call on the world’s governments to come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules, and get to work implementing them.

Such a [set of binding rules set forth in a] convention should commit governments to avoiding cyberattacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that governments assist private sector efforts to detect, contain, respond to, and recover from these events, and should mandate that governments report vulnerabilities to vendors rather than stockpile, sell, or exploit them.

8. As of August 2023, it appeared that the following text was under discussion in the WTO Joint Statement Initiative (JSI) on e-commerce [[8]](#footnote-8):

C.4 Cybersecurity

*Co-convenors' note: Small group discussions on this topic were concluded in October 2022. Co-convenors and the facilitator remain available for discussion with any interested delegations.*

1. The [Parties/Members] recognize that threats to [cybersecurity/information security] undermine confidence in [digital trade/electronic commerce].

2. The [Parties/Members] recognize the evolving nature of cyber threats. In order to identify and mitigate those threats and thereby facilitate [digital trade/electronic commerce] the [Parties/Members] shall endeavor to:

(a) build the capabilities of their respective nation entities responsible for cybersecurity incident response;

(b) collaborate to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks[of [Parties/Members] and to address cybersecurity incidents in a timely manner, [combat cybercrime], as well as to share information for awareness and best practices.

3. Given the evolving nature of cyber threats and their negative impact on [electronic commerce/digital trade], the [Parties/Members] recognize the importance of risk [-based/management] approaches in addressing those threats while minimizing trade barriers. Accordingly, [where appropriate] each [Party/Member] shall endeavor to employ, and to encourage enterprises within its jurisdiction to use, risk [-based/management] approaches that rely on risk management best practices and on standards developed in a consensus-based, transparent, and open manner, to identify and protect against cybersecurity risks, to detect [cybersecurity events], and to respond to and recover from cybersecurity incidents.

*Drafting note: The delegations’ understanding of standards developed in a consensus-based manner draws on the TBT Committee Principles for the Development of International Standards, Guides and Recommendations. In this context, consensus need not imply unanimity.*

9. As can be seen, the provision being discussed in the WTO JSI in 2022 is far more detailed and prescriptive than the provision in the 2012 ITRs. (The reference to “Principles for the Development of International Standards, Guides and Recommendations” appears to refer to this text: <https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm> )

10. Thus it appears that many Member States, in particular developed countries, are of the view that binding treaty-level provisions regarding cybersecurity are needed, and that they should be more detailed than the generic provision found in the 2012 ITRs.

11. Indeed, in September 2022, the European Commission published a proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, whose intent is to bolster cybersecurity rules to ensure more secure hardware and software products.[[9]](#footnote-9)

12. It is worth noting that one of the topics under discussion in the WTO JSI is whether to refer to “cybersecurity” – which has traditionally been used to refer to the non-content related technical aspects of ICT security, such as confidentiality and authentication – or to “information security” – which has traditionally been used within the United Nations to refer also to content-related aspects of ICT security, such as combating so-called disinformation[[10]](#footnote-10).

13. Consequently, it appears that agreement on treaty-level provisions regarding cybersecurity is a new trend and/or and emerging issue in telecommunications/ICTs and its environment. (This has lead to comments from civil society[[11]](#footnote-11), [[12]](#footnote-12), [[13]](#footnote-13).)

14. Further, since new provisions are being proposed/agreed, it appears that the provisions of the 2012 ITRs do not provide appropriate high-level guiding principles in the current telecommunication/ICT environment.

15. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs. In particular, Member States may wish to consider the following possible commitments[[14]](#footnote-14):

1. Parties shall refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes.
2. Parties shall refrain from using ICTs to steal the intellectual property of private companies, including trade secrets or other confidential business information, and to provide competitive advantage to other companies or commercial sectors.
3. Parties shall refrain from inserting or requiring “backdoors” in mass-market commercial technology products.
4. Parties shall agree to a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities that reflects a strong mandate to report them to vendors in mass-market products and services.
5. Parties shall exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise, and not reusable; Parties shall also ensure that they maintain control of their weapons in a secure environment.
6. Parties shall agree to limit proliferation of cyber weapons; governments shall endeavor not to distribute, or permit others to distribute, cyber weapons and to use intelligence, law enforcement, and financial sanctions tools against those who do.
7. Parties shall limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.
8. Parties shall endeavor to assist private sector efforts to detect, contain, respond, and recover in the face of cyberattacks; in particular, they shall enable the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs); intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals.
9. Parties shall facilitate the establishment of an international cyberattack attribution organization to strengthen trust online.
10. Parties shall, individually and in cooperation, develop and apply measures to increase stability and security of international telecommunication networks and in the use of ICTs in order to achieve effective use thereof and avoidance of technical harm thereto, as well as to maintain international peace and security, the harmonious development of ICTs, and to prevent ICT practices that may pose threats to international peace and security.[[15]](#footnote-15)
11. In case of ICT incidents, Parties shall consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.
12. Parties shall not knowingly allow their territory to be used for internationally wrongful acts using ICTs.
13. Parties shall consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats.
14. Parties shall not conduct or knowingly support ICT activity contrary to their obligations under international law, that intentionally damages critical infrastructure, or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
15. Parties shall take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly Resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.
16. Parties shall respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts; they shall also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.
17. Parties shall take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products; they shall prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
18. Parties shall encourage responsible reporting of ICT vulnerabilities, and share associated information on available remedies to such vulnerabilities, to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.
19. Parties shall not conduct, or knowingly support, activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State; a Party shall not use authorized emergency response teams to engage in malicious international activity.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. <https://www.itu.int/md/S23-CL-C-0121/en> [↑](#footnote-ref-1)
2. Hill, Richard (2013) ["WCIT: failure or success, impasse or way forward?"](http://ijlit.oxfordjournals.org/content/21/3/313.abstract), *International Journal of Law and Information Technology,* vol. 21 no. 3, p. 313,  DOI:10.1093/ijlit/eat008 [↑](#footnote-ref-2)
3. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 75 [↑](#footnote-ref-3)
4. <https://www.schneier.com/blog/archives/2007/01/information_sec_1.html>; a comprehensive discussion is given in pages 103-107 of the Global Internet Report 2016 of the Internet Society, see in particular the examples on p. 101. The Report is available at: <https://www.internetsociety.org/globalinternetreport/2016/>. See also item 5 on page 8 of: <https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf>. [↑](#footnote-ref-4)
5. ISOC (2016) <https://future.internetsociety.org/2016/index.html>. [↑](#footnote-ref-5)
6. Indeed, there have been calls for such minimum standards. See for example sections 2.1 and 2.3 of <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity>; pages 109 ff. of the Legislative Proposals of the US Cyberspace Solarium Committee, available at: <https://www.solarium.gov/>; and pages 15-21 of the “Cybersecurity Lessons from the Pandemic: Legislative Proposals”, same web site. [↑](#footnote-ref-6)
7. <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4>. [↑](#footnote-ref-7)
8. <https://www.bilaterals.org/?wto-2023-plurilateral-ecommerce-48862> [↑](#footnote-ref-8)
9. <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act> . A detailed commentary of this proposal can be found here: <https://berthub.eu/articles/posts/eu-cra-secure-coding-solution/> [↑](#footnote-ref-9)
10. See <https://disarmament.unoda.org/ict-security/> [↑](#footnote-ref-10)
11. <https://www.newsclick.in/Why-Spam-Trade-Issue-Suits-Dominant-Developed-Countries> [↑](#footnote-ref-11)
12. <http://apig.ch/WTO%20ITU%20overlaps%20paper.pdf> [↑](#footnote-ref-12)
13. Hill, Richard (2020) “[A New Convention for Data and Cyberspace](https://itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/)”, in the call for a [Digital New Deal](https://itforchange.net/digital-new-deal/) (October 2020) [↑](#footnote-ref-13)
14. Taken from 3.11 of:  
     <https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/> [↑](#footnote-ref-14)
15. This and the following provisions are based on the eleven norms of paragraph 13 of the 2015 Report of the UN Intergovernmental Group of Experts in the Field of Information and Telecommunications in the Context of International Security (UN document A/70/174), and on the 2012 International Telecommunication Regulation. [↑](#footnote-ref-15)