Digital standardization, cybersecurity issues and international trade law

Alberto Oddenino[*]

1. *Introduction*

National and international digital standards are having a growing impact on international trade law. The traditionally most evident dimension of the extensive activity of standard-setting bodies in relation to the functioning of the Internet is related to openness and interoperability, which are to be considered as core values in the development of the Internet and the Digital Trade Agenda.

Against this background, the need for cybersecurity prompts State control over the Internet and affects trade liberalization, triggering the exception of national security. National standards therefore become an instrument of protection of the national interest, whose broad interpretation provides a powerful protectionist tool.

If new trade agreements are to consider these issues more directly, it is necessary to deal with cybersecurity in the context of the World Trade Organization (WTO), finding viable solutions through an evolutionary interpretation, in particular, of the Agreement on Technical Barriers to Trade (TBT).

For a smooth functioning of TBT, a shared development of international standards is needed, based on a public-private partnership that should aim at overcoming competition of standards and fragmentation, which could negatively impact the very structure of the Internet.

Following this line, cybersecurity could become a foundational element of trust for digital trade. Rather than serving as a means to advocate

[*] Professor of International Law, University of Turin, Department of Law.

for national interests, it could become not opposite but complimentary to openness.

International standards could therefore provide a viable solution to foster the development of international digital trade in the existing framework of the WTO, serving cybersecurity issues without disregarding the principle of technological neutrality and the logic of openness and interoperability.

To develop these assumptions, this article will first introduce the concepts of interoperability and standardization, then moving to cybersecurity and its impact on international trade law, with particular reference to the WTO system and finally focusing on the actual and potential role for international digital standardization, in its public-private partnership dimension.

2. *Interoperability, digital standardization and their seminal role for ICT*

As clarified by the International Organization for Standardization (ISO), technical standards are documents that establish engineering norms for products or processes.[1] In general, international trade lawyers agree that regulatory barriers to trade would be minimized should regulatory harmonization (or at least regulatory cooperation) be improved,[2] also through the adoption of shared technical standards.

Particularly in Information and Communications Technology (ICT), where normative and technical dimensions are interwoven or even merged, standards are increasingly seen as an alternative to the use of international law and treaties to deal with digital issues and in particular

[1] Indeed, a technical standard is a 'document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context' *and* 'based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits' (cf International Standards Organization, *Guide on standardization and related activities-general vocabulary* (2004) <www.iso.org/obp/ui/#iso:std:iso-iec:guide:2:ed-8:v1:en>).

[2] See N Mishra, 'International Trade, Internet Governance and the Shaping of the Digital Economy' (2017) ARTNeT Working Paper Series no 168, 9 <https://artnet.unescap.org/publications/working-papers/international-trade-internet-governance-and-shaping-digital-economy>.

issues of cybersecurity.[3] Common technical standards are a sort of postulate for ICT and indeed they function as economic infrastructure capable of reducing barriers to the dissemination of technological innovation. The result is to increase consumer welfare by ensuring technical interoperability among products made by different producers.[4]

The relevant literature suggests that social and economic benefits of standardization may include, *inter alia*, (*i*) lower costs thanks to the simplification of complex processes, (*ii*) lower learning costs for new producers, (*iii*) increased possibility for producers to exploit economies of scale, (*iv*) lower transaction costs between transacting parties, (*v*) higher market information and confidence by signaling product quality, or the compatibility of products or components, (*vi*) lower compliance costs, (*vii*) increased competition among producers and therefore (*viii*) lower prices to consumers.[5]

The underlying rationale is openness and interoperability, because the potential for revolutionary technologies to change the way we live and work depends largely on their ability to communicate with each other. Global and supranational markets are indeed increasingly defined by ICT interoperability standards. No wonder that the EU Commission has long ago identified a lack of interoperability as one of the most significant obstacles to the virtuous cycle of digitalization,[6] so that effective interoperability between networks, devices, applications, data repositories and services has ever since become one of the fundamental pillars of the so-called European Digital Agenda.[7] From this perspective, the continuous growth of technologies requires a new paradigm, necessarily characterized by a growing level of openness and interoperability. Such needs have

[3] For a general assessment of the normative role of standardisation and the theoretical relationship with the sources of international law see Y Radi, *La standardisation et le droit international. Contours d'une théorie dialectique de la formation du droit* (Bruylant 2013).

[4] See M Finnemore, DB Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110 AJIL 425, 437.

[5] See JK Winn, 'Governance of Global Mobile Money Networks: The Role of Technical Standards' (2013) 8 Washington J L Technology & Arts 197, 216.

[6] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe' COM(2010)245 final, 3.

[7] See also W Kerber, H Schweitzer, 'Interoperability in the Digital Economy' (2017) 8 J Intellectual Property, Information Technology & Electronic Commerce L 39.

resulted in an increased attention paid to standardization, which features prominently in the legislative and political agenda of the EU and US.[8]

Standard-setting processes such as those conducted under the auspices of the ISO or the Internet Engineering Task Force (IETF) are among the most effective solutions in order to achieve technical interoperability.[9] As is well known, international governmental organizations are generally established to better pursue goals and activities which are international in nature, because their reach goes beyond national borders. To that effect, some of them may have full authority to establish binding rules. More often, they set rules which do not amount to binding obligations, being framed in terms of *soft law* susceptible of voluntary acceptance.

In particular, technical standards are nonbinding rules of great effectiveness because they bear a high level of spontaneous compliance. In this perspective, it is particularly evident that a strict opposition between binding and non-binding norms proves evanescent if not misleading. As voluntary standards are perceived as the appropriate international practice to deal with particular issues, in cooperation with other States and relevant actors, it is indeed unusual for States and other stakeholders to decide not to abide by them.[10]

This is precisely the essence of openness in international technical standards aimed at creating shared and open innovation, which is vital for the development of ICT.[11] Against this background, it is necessary to

[8] Accordingly, '[t]his shift suggests the adoption of a broader definition of open innovation, focused not only on the sharing of technological breakthroughs, but also on the sharing of data and models within the industry, as well as with consumers, authorities and other interested third parties' (see S Barazza, "'Let Me Talk to You': Open Standards and the Technologies of the Future' (2018) 13 J Intellectual Property L & Practice 167).

[9] Indeed, the 'governance of technical standard-setting processes and managing the 'interface' between national laws and technical standards are fundamental tasks that must be accomplished in order for any global market to function at an operational level' (cf Winn (n 5) 203).

[10] For a critical assessment of the role of soft law in the international legal order and for a useful distinction of the formal and the substantial dimension of the divide between hard and soft law see J d'Aspremont, 'Softness in International Law: A Self-Serving Quest for New Legal Materials' (2008) 19 Eur J Int L 1075.

[11] See AD Sofaer, D Clark, W Diffie, 'Cyber Security and International Agreements' (2010) Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy 179, 198.

evaluate how cybersecurity issues may affect these general assumptions on open standards.

3. *Cybersecurity and its ambiguous status in the context of Digital Trade*

Interoperability and openness cannot be considered in isolation from cybersecurity. These issues are indeed two sides of the same coin. Global cybersecurity implicates a range of economic, privacy, and national security issues. As a matter of principle, there are two main general categories of cybersecurity issues: on the one hand, there are actions aiming at damaging a cyber system ('cyberattacks'); on the other hand, there are actions aiming at exploiting the cyber infrastructure for unlawful purposes without damaging that infrastructure ('cyber exploitation').[12]

Given the millions of lines of code involved in modern programming, vulnerabilities are an inherent feature of cyberspace so that indeed there can be no such thing as 'zero risk' in cybersecurity.[13]

Cyber insecurity stems from the fact that cyber systems, as seen with reference to openness and interoperability, have been designed to facilitate access and utilization rather than security. The fact that we live in a hyper-connected world, where plenty of smart devices and objects are connected implies that the question is to determine the level of risk which shall be accepted and, therefore, does not amount to a danger to 'essential interests'.[14]

International cooperation and the execution of international agreements can certainly enhance cybersecurity. This is why the UN began discussing cybersecurity issues as early as 1998 when resolution 53/70 was passed.[15] Yet in 2015, National Security Strategy report by the Obama administration argued that cybersecurity requires observed international norms and a shared responsibility among States, while at the

[12] ibid 181.

[13] See Finnemore, Hollis (n 4) 432.

[14] See S Peng, 'Cybersecurity Threats and the WTO National Security Exceptions' (2015) 18 J Intl Economic L 449, 470.

[15] See UNGA res 53/70 'Developments in the field of information and telecommunications in the context of international security' (4 December 1998) UN Doc A/RES/53/70.

same time declaring that 'the United States has a special responsibility to lead a networked world'.[16]

This reveals how in principle States tend to acknowledge the global nature of cybersecurity challenges while at the same time in practice they show a general tendency to regulate cybersecurity issues at the national level.

The result is that there are no comprehensive frameworks of international rules trying to harmonize national systems, with the only exception being the Budapest Convention, which attempts to harmonize national criminal laws concerning cybercrime.[17]

This situation leads to a paradox. Cybersecurity is at the same time a postulate for realizing the Digital Trade Agenda and one of the most widespread barriers that States are inclined to build for protectionist purposes.

Consequently, it is necessary to examine cybersecurity in the context of international trade law, both from the general systemic perspective of WTO law and from the perspective of national interest exceptions.

4. *Cybersecurity in the context of international trade*

The Internet and ICT are capable of offering more benefits to the development of global trade than any single policy has ever managed to achieve. In this vein, it cannot be denied that the digital economy cannot keep growing unless the Internet remains an open, stable, secure and trustworthy environment[18]. Within this perspective, national measures implemented in order to ensure cybersecurity should only be justified if they comply with exceptions expressly provided by international trade agreements.

It must be outlined that until recently, there were virtually no international trade agreement dealing directly with cybersecurity issues (let

[16] See SS Malawer, 'Chinese Economic Cyber Espionage: U.S. Litigation in the WTO and Other Diplomatic Remedies' (2015) 16 Georgetown J Intl Affairs 158, 159, with the reference to the Executive office of the President of the United States, National Security Strategy (February 2015).

[17] Council of Europe, Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) CETS no 185.

[18] For further references see Mishra (n 2) 18.

alone trying to regulate them). Although this essentially holds true even today, it should be observed that, in the last few years, States have begun to include in international trade agreements specific chapters containing binding rules aiming at preventing contracting States from interfering with digital data flows.[19] In order to work properly and achieve their aims, these chapters often include also other specific legal requirements on cybersecurity[20] (or other connected issues). It has been observed that the incorporation of Internet policy issues in international trade agreements is basically an attempt to cope with an ever-increasing necessity for regulatory coordination and cooperation between States on areas that impact international trade, while also having a deep impact on the process of Internet governance.[21] For this reason the main framework of reference still is WTO.

4.1. *Cybersecurity in the framework of WTO: The role of TBT*

To tackle the risk of digital protectionism, cybersecurity issues should be framed in the context of the WTO system and, in particular, cybersecurity standards should be evaluated in the context of the TBT. In fact, as cybersecurity standards often qualify as data localization measures, they produce a number of effects on the liberalization of trade. Therefore, one way to tackle problems arising from conflicting national standards and to foster interoperability may lie in the application of TBT rules.

As it is well known, TBT in principle covers technical product regulations which are not covered by the Sanitary and Phytosanitary Measures Agreement (SPS).[22] Technical regulations may be adopted in the pursuance of objectives of public policy, generally indicated in recital 6 of the Preamble of the TBT.[23] However, the agreement is based on the ambiv-

[19] See, for example, the Electronic Commerce Chapter of the Trans-Pacific Partnership Agreement.

[20] See for example art 14.16 of the TPP, setting out a provision on cybersecurity cooperation among member countries.

[21] See Mishra (n 2) 5.

[22] See generally T Epps, M Trebilcock, *Reserach Handbook on the WTO and Technical Barriers to Trade* (Edward Elgar 2013).

[23] The TBT Preamble states that 'no country should be prevented from taking measures necessary to ensure the *quality of its exports*, or for the *protection of human, animal or plant life or health, of the environment, or for the prevention of deceptive*

alence of technical regulations, standards and conformity assessment procedures. On the one hand, standardization serves diverse positive goals, by capturing network externalities and reducing information asymmetries.[24] On the other hand, technical regulations adopted at the national level may disguise the intention to protect national industry. Consistently, TBT includes the basic principle that standards and technical regulations are considered illegitimate only when they constitute an unnecessary restriction on trade.[25]

Generally, the TBT has been considered as mainly related to trade in goods. Thus, the application of TBT rules to cybersecurity standards could raise the issue of qualification of digital trade and digital products for establishing the applicable trade law regime.[26] However, recent practice shows an increasing reference to TBT rules when it comes to cybersecurity national measures. The TBT Committee has already discussed the matter in various meetings, in which several WTO Members have highlighted the risk that cybersecurity national standards may hinder international trade in ICT products.

The rise of specific trade concerns (STCs) in relation to China's cybersecurity measures confirms that WTO Members are already considering the TBT applicable to these kinds of standards.[27] The rationale and the nature of cybersecurity standards and regulations, as previously highlighted, shed some light on the relevance of TBT rules in this particular

practices, at the levels it considers appropriate, subject to the requirement that they are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail or a disguised restriction on international trade, and are otherwise in accordance with the provisions of this Agreement' (emphasis added).

[24] See M Koebele, 'Preamble TBT', in R Wolfrum, P-T Stoll, A Seibert-Fohr (eds), *WTO – Technical Barriers and SPS Measures (Max Planck Commentaries on World Trade Law)* (Martinus Nijhoff 2007) 173.

[25] See recital 5 of the Preamble of the TBT.

[26] For a discussion on the nature of digital products and the applicable trade rules see S Fleuter, 'The Role of Digital Products Under the WTO: A New Framework for GATT and GATS Classification' (2016) 17 Chicago J Intl L 153 ff; F Farrokhnia, C Richards, 'E-Commerce Products Under the World Trade Organization Agreements: Goods, Services, Both or Neither? (2016) 50 J World Trade 793 ff. The stalemate of WTO negotiations on the issue of digital trade finds its origin in the competing approaches of the US and the EU. See generally S Wunsch-Vincent, *The WTO, the Internet and Trade in Digital Products: EC-US Perspectives* (OUP 2006) 51 ff.

[27] See Committee on Technical Barriers to Trade, *Minutes of the Meeting of 14-15 June 2017*, Doc G/TBT/M/72 (25 September 2017) 2-4.

context and show the possibility of using international trade obligations in order to balance conflicting national interests.

This is also due to the particular content of TBT obligations, which are worth recalling. In particular, under Article 2.1 of the agreement, Member States are required to accord to other countries, by means of technical regulation,[28] a treatment no less favourable than like products produced domestically. Moreover, Member States are also obliged to ensure that technical regulations and standards are not more trade-restrictive than necessary to fulfil a pursued legitimate objective.[29]

However, for our purposes, the most relevant rule of the TBT is the one concerning the preference for international standards over national ones. According to Article 2.4 in fact, when a technical regulation is required and relevant international standards are available, Members shall use them as the basis for their own internal regulation, unless these international standards prove to be ineffective in light of the objective pursued, due to geographical and climatic factors or to '*fundamental technological problems*'. Upon request of other Members, the regulating State is also under the duty to state reasons for not applying the available international standards.[30] International standards therefore become an essential basis for the internal regulation, meaning that they must be used '*as the principal constituent or fundamental principle for the purpose of enacting the technical regulation*'.[31]

This provision is generally interpreted as the acknowledgement of a pivotal role of international standards in the WTO system. More precisely their primacy is at the core of the TBT, which seeks the harmonization of different domestic standards in order to improve the efficiency of production and to facilitate international trade.

Besides substantial obligations on technical regulation, the TBT sets forth certain transparency obligations that may be at odds with the very

[28] On the definition of technical regulation see WTO Appellate Body, *European Communities – Measures Prohibiting the Importation and the Marketing of Seal Products*, Doc WT/DS400-401/AB/R (22 May 2014) paras 5.16 ff.

[29] The necessity test incorporated in the TBT follows the same pattern of the one related to general exceptions under art XX GATT.

[30] TBT, art 2.5.

[31] Hence, it is not necessary for national regulator bodies to enact a regulation entirely identical to the relevant international standards. See WTO Appellate Body, *European Communities – Trade Description of Sardines*, Doc WT/DS231/AB/R (26 September 2002) paras 240 ff.

nature of cybersecurity national measures. Under Article 2.9.2 and under Article 2.10.1, Member States are required to notify draft technical regulations (or regulations already adopted for matters of urgency) when two conditions are present: first, when an international standard does not exist or the domestic regulation is in contrast with relevant international standards; secondly, when the national regulation may produce a significant effect on the trade of other Member States.[32] Moreover, Member States adopting national technical regulations must also publish a related notice at an 'early appropriate stage'.

4.2 *Cybersecurity, national interest clause and WTO*

As mentioned, the possibility for States to foster cybersecurity through national measures cannot be seriously contested: just as everyone would expect States to defend their citizens against enemy aircraft rather than leaving such task to each individual, no one would expect that States should behave differently in the realm cyberspace.[33]

It should be noted, however, that domestic regulations on Internet-related issues – including cybersecurity – are often adopted and enforced by national legislators without taking into consideration the global nature of cyberspace. Two connected aspects which are often neglected are that cybersecurity issues also relate to international trade and, therefore, that national measures aiming to enhance cybersecurity are inherently relevant for international trade law.[34]

Within the WTO legal order, States have the possibility of not complying with their international legal obligations, if necessary, to protect their 'essential security interests'.[35] Issues arise mainly because, under the WTO, such national security exceptions are so-called 'self-judging'

[32] See L Tamiotti, 'Article 2 TBT', in R Wolfrum, P-T Stoll, A Seibert-Fohr (eds), *WTO – Technical Barriers and SPS Measures (Max Planck Commentaries on World Trade Law)* (Martinus Nijhoff 2007) 230.

[33] See P Rosenzweig, 'The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence' (2010) Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy.

[34] For further references see N Mishra (n 2) 18.

[35] See for example art XXI of the GATT, art XIV bis of the GATS, art 73 of the TRIPS, and art XXIII of the GPA.

clauses, meaning that the decision on what represents an essential security interest as well as the decision on which measures are necessary to cope and protect such essential security interest are basically left to the WTO Member State that invokes the applicability of the clause.[36] It comes as no surprise that these exceptions can be easily used by WTO Member States as a pretext for protectionist purposes.

The national interest exceptions have not prevented the capacity of the WTO regime to operate effectively. This is probably due to the fact that WTO Member States appear to have exercised those rights with caution and restraint, perhaps knowing that such clauses are equally available to all parties so that an extensive interpretation is in the interest of none of them. An indirect consequence of such restraint is that the practice (*rectius*, the lack thereof) under both the GATT and the WTO does not resolve the issue as to whether (let alone to what extent) a national security exception could be reviewable by a panel.[37]

This is relevant because it has been observed that potential tensions with the national interests exception are especially – although not solely[38] – likely to arise in connection with the creation of cyber norms and standards.[39] In the last few years, for example, several States have indeed adopted national measures restricting cross-border data flows and including measures aimed also at improving the enforcement of domestic cybersecurity regulations or standards. Given the purposes for which cybersecurity standards are adopted at the national level, transparency obligations might not be complied with in order to safeguard underlying national security interests, nor would their content be published in its entirety.

[36] See P Van Den Bossche, The Law and Policy of the World Trade Organization (2nd edn, CUP 2008) 664.

[37] For further reference see Peng (n 14) 459-462.

[38] For example, also the recent decisions to impose tariffs and taxes on steel and aluminium imports within the US taken by the Trump administration has been argued to fall under art XXI of the WTO Agreement.

[39] It has been observed that 'sharing information is a fundamental characteristic and benefit of transnational regimes and would be an important aspect of any cyber-security agreement. A government may occasionally be faced, however, with a situation in which sharing information related to a cyber threat could prejudice its security by, for example, revealing vulnerabilities or defensive plans to a State or non-state actor suspected of supporting cyberattacks. States should be permitted, in their discretion, to invoke a national security exception in all such situations' (cf Sofaer, Clark, Diffie (n 11) 195.

A clear example is Chinese data security law, entered into force in 2017. It is considered one of the most complex and far-reaching of national cybersecurity legislations.[40] As it relates to transparency in particular, the establishment of broad discretionary powers for the authorities in charge of the 'security review' of foreign ICT operators raises serious doubts of compatibility with WTO rules. Consequently, various Members have requested that China clarify the scope of such review assessments and the functioning of the connected procedures.[41]

A further example, not pursued before the WTO, relates to Canada and a bidding process run in 2012 to consolidate the governmental many non-interoperable email platforms into a single system. Canada, a signatory to the WTO Agreement on Government Procurement (GPA), introduced several measures that could be seen as discriminatory, including limiting bids to Canadian firms or Canadian subsidiaries, and requiring that support personnel must be Canadian citizens. Canada recognized that such requirements did not comply with the GPA but insisted that the national priority was sought in order 'to create a secure, centralized communications infrastructure,' and thus it invoked the national security exception provided by such trade agreements.[42]

As already recalled, no WTO cases have ever involved a security exception.[43] This situation may change considering that, earlier this year,[44] the United States informed the WTO that China's data network restrictions that entered into force in March 2018 appear to create illegal restrictions for cross-border service supplies and needs to be addressed by the WTO.[45] The Chinese government has replied that the challenged

[40] See T Schmitt, 'China's Great Firewall Remains Shut to Noncompliant U.S. Tech Firms' (15 January 2018) Georgetown J Intl L Online <www.gjil.org/2018/01/chinas-great-firewall-remains-shut-to.html>.

[41] Committee on Technical Barriers to Trade, *Minutes of the Meeting of 14-15 June 2017* (n 26) 2.

[42] See AA Friedman, 'Cybersecurity and Trade: National Policies, Global and Local Consequences' (2013) Center for Technology and Innovation at Brookings 5 <www.brookings.edu/wp-content/uploads/2016/06/BrookingsCybersecurityNEW.pdf>.

[43] See Malawer (n 15) 161.

[44] Communication from the United States to the WTO of 23 February 2018 available on the WTO's website.

[45] More specifically, the US statement 'claimed that new Chinese regulations would prohibit Virtual Private Networks (VPN) and leased lines from connecting across the Chinese border' (cf T Schmitt, 'United States Flags China's VPN Ban as Possible WTO

national measure does comply with WTO rules because it protects the general interest of the Chinese public, ensuring that foreign companies do not do any harm to Chinese national security and national consumers' interests.

Potential clashes between national legislation and international commitments of the enacting States have been recently highlighted and discussed at the WTO level also with regard to the draft of the cybersecurity law proposed by Vietnam in 2017.[46] Several WTO Member States indeed expressed concern that such measure could have an adverse effect on trade.

In this vein it has been noted that national interest clauses should be interpreted in good faith.[47] The principle of good faith qualifies as a general principle of international law pursuant to Article 38(1)(c) of the Statute of the International Court of Justice.[48] Good faith interpretation is described as a two-stage process, composed of both an objective and a subjective level of scrutiny.[49] In particular, applying the general principle of good faith to a self-judging clause such as the national interest clause would require ascertaining whether the State is genuinely convinced that the national measure not compliant with the international obligations of the State is adequate and necessary to protect an essential security interest.[50]

Overcoming the self judgement is therefore a complex task and it would imply an awkward test on subjective good faith, which is a very

Violation' (2018) Georgetown Law Technology Rev <www.georgetownlawtechreview.org/united-states-flags-chinas-vpn-ban-as-possible-wto-violation/GLTR-03-2018/>).

[46] For example, art 34 of the draft law specifies that '[f]oreign firms providing telecommunication and Internet services in Vietnam shall comply with Vietnamese regulations, respect national sovereignty, interests and security, user interests, obtain licenses, locate their representative offices and servers in Vietnam, and secure user data and accounts', while however according to WTO rules, foreign telecommunication and Internet service providers cannot be required to locate their representative offices in a given country.

[47] See Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 31 January 1980) 1155 UNTS 331 (VCLT) art 26.

[48] See AD Mitchell, M Sornarajah, T Voon, *Good Faith and International Economic Law* (OUP 2015).

[49] See M Panizzon, *Good Faith in the Jurisprudence of the WTO* (Hart 2007) 203.

[50] See Peng (n 14) 466.

difficult element to demonstrate.[51] This prompts for a more thorough consideration of the role of international digital standards for dealing with cybersecurity issues in the context of WTO.

5. *The role of international cybersecurity standards*

As it has been highlighted, cybersecurity plays a paradoxical role in international trade. On the one hand, domestic measures adopted in order to ensure cybersecurity at the national level may have the effect – if not the object – to hamper international trade. At the same time, however, international trade would be hampered just as much by a lack of confidence in Internet security, as a high degree of Internet security is a prerequisite to facilitate digital economic transactions.

A possible effective solution is offered by the adoption of international technical standards, which may contribute to increasing the degree of confidence in Internet security. It is therefore not surprising that, within the last decade, standard-setting bodies have engaged in extensive activity in relation to the functioning of the Internet.

The harmonization of cybersecurity standards, fostered by TBT obligations, may also support an open Internet and reduce costs of Internet access, especially in developing countries. Several international standard setting bodies, such as ICANN and ETSI, have already addressed various issues of cybersecurity regulations.[52] Nonetheless, for the TBT obligations to become applicable, international standardizing bodies must

[51] Indeed, the interpretive use of good faith in its subjective dimension proves difficult to apply effectively. As far as the existence of an essential security interest to protect from potential cybersecurity breaches is concerned, it is irrelevant whether, objectively speaking, the ICT system or the ICT infrastructure that the national measure aims at protecting are actually indispensable for security. What is relevant is whether the WTO Member State claiming the application of the national interest clause genuinely considers the enacted restriction to be adequate and necessary for the purposes of protecting an ICT system or an ICT infrastructure whose protection such State genuinely considers to be indispensable for security. This subjective level of scrutiny proves insufficient to tackle the risk of a purely unilateral use of the exception. On the weaknesses of a merely subjective use of the general principle of good faith in treaty interpretation see A Oddenino, *Buona fede e Pacta sunt servanda nell'applicazione dei trattati internazionali* (Giappichelli 2003) 97 ff.

[52] See recently the ETSI position paper on draft EU Regulation 2017/0225, available at <www.etsi.org/images/files/ETSI_position_paper-CyberAct_20180206.pdf>.

guarantee a certain level of participation by WTO Member States. In the *US – Tuna Labelling (II)* case, for instance, the Appellate Body recognized that the Agreement on International Dolphin Conservation Program (AIDCP), which would have permitted an alternative labelling on the part of the US, could not be considered as an international standardizing body, since WTO Members can only accede by way of invitation.[53] The same reasoning can be applied to other bodies currently dealing with digital standards, such as the Organisation for Economic Co-operation and Development (OECD).[54]

In the context of digital trade and cybersecurity measures, however, this mechanism may become particularly complex because of the way standards are created and developed, often by a joint cooperation between public and private bodies, in a context of great fragmentation.[55]

In this vein, it should be underscored that private entities play major roles in the cybersecurity arena: technical standards are indeed developed and proposed mostly by non-governmental bodies,[56] with the aim of enhancing cybersecurity.[57] Examples include, among others, norms for Internet service providers, hardware manufacturers, and software developers.[58]

[53] See WTO Appellate Body Decision, *US – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, Doc WT/DS381/AB/R (16 May 2012) para 374.

[54] See JP Meltzer, 'A New Digital Trade Agenda, E15Initiative' International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum (Geneva, 2015) 11 <http://e15initiative.org/publications/a-new-digital-trade-agenda/>.

[55] See W Liu, 'International Standards in Flux: A Balkanized ICT Standard-setting Paradigm and its Implications for the WTO' (2014) 17 J Intl Economic L 561, 568.

[56] Indeed, '[m]ultistakeholder processes like NETmundial (which involved NGOs, firms, and individuals) or the Montevideo Statement (which was signed by the major Internet institutions) suggest that the political basis of propriety can also arise among actors other than states' (cf Finnemore, Hollis (n 4) 442).

[57] See Sofaer, Clark, Diffie (n 11) 182-183.

[58] On the extremely complex framework of reference for standard-setting and cybersecurity see Winn (n 5) 217-218, explaining that '[f]ormal public international standard-setting organizations that may have jurisdiction over ICT technical standards include the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU); each of these organizations has a formal, public counterpart in each country that chooses to participate in them. While the processes used by these global technical standard-setting organizations seek to be transparent and inclusive, they may also be slow, bureaucratic, and out of touch with conditions in the markets in which the standards are to be implemented (…). In order to ensure that ICT standard development can keep pace with rapid technological innovation in global ICT markets, new forms of private

In light of the above, the digital world largely operates without any formal international institution having the competence to set standards or practices. The digital world is indeed based on *standards*, but the term is often used to indicate something quite different from a rule adopted by an international governmental organization. Significant aspects of the inadequate level of security in cyber operations may stem from the limits to what can be achieved using informal organizations with no power to adopt even 'soft law' rules.

To be sure, cyberspace provides a particularly clear example of how the effectiveness of a given rule does not necessarily depend solely on the public or private nature of the actor that adopts it. Market power can sometimes replace legal authority, and this is especially so in the digital sectors. If a technical standard is adopted by an association of undertakings with enough market power, national regulators may find themselves bound to decide between two alternatives. The first is permitting their citizens to access the services offered according to the adopted standards; the second is exercising regulatory authority bearing the risk of preventing their citizens from being able to enjoy the service at stake should the market operators decide that it is not worth it to comply with the domestic technical standards adopted in that specific jurisdiction (for example because of the size of the national market). In other words, once a platform based on global ICT networks takes root within a domestic economy, regulators may find it difficult to mandate changes in the way the platform operates.[59]

The depicted situation is consistent with Internet Governance ambiguities and with the unclear status of it, and of cybersecurity principles,

international standard-developing organizations known as "consortia" or "fora" have emerged in recent years. These new ICT SDOs range in size from a small handful of members working closely together to thousands of members scattered around the world collaborating by means of Internet communications. The Internet Engineering Task Force (IETF), developer of the Transmission Control Protocol/Internet Protocol (TCP/IP) standard which defines the Internet, and the World Wide Web Consortium (W3C) are examples of large, informal ICT standard-developing organizations with members around the world. By contrast, EMVCo, the ICT SDO for the European EMV payments standard, has only four members: American Express, JCB, MasterCard, and Visa. Informal private ICT SDOs are often referred to as consortia, and because they are generally exempt from regulation by national governments, they can often develop standards more quickly and efficiently than formal, public ICT SDOs'.

[59] See Winn (n 5) 226.

in the context of public international law.[60] It has been suggested that the adoption of resolutions and recommendations by intergovernmental organizations on issues related to internet governance such as cybersecurity, marks a 'policy shift' towards a 'soft law approach';[61] such shift is addressed to the internet multistakeholder community as a whole constituting of States, businesses, and the civil society. Therefore, the development of protocols or standards on cybersecurity, and management of security risks requires collaboration amongst different stakeholders and particularly of the private sector.

While it has been observed that a system based on the actions of private actors could prove to be more adequate than traditional mechanisms based on the adoption of standards by public international regulators, it has also been argued that

> '[t]he current, de facto distribution of power appears to have ignited a competition for influence likely to disrupt rather than to enhance cyber security. An agreed redistribution of responsibilities that is acceptable to all stakeholders could ensure constructive cooperation in a highly complex undertaking'.[62]

This shows the difficulty of striking a fair balance between the public and the private elements of the complex process of digital standard setting. As recently underscored in reference to the role of standard setting in WTO system more broadly, the core issue is then determining the

[60] There is a growing literature on the ambiguous status of Internet Governance in International Law. See in general K Kittichaisaree, *Public International Law of Cyberspace* (Springer 2017). In Italian doctrine see, also for further reference, A Oddenino, *La governance di internet fra autoregolazione, sovranità statale e diritto internazionale* (Giappichelli 2008); G Ruotolo, *Internet-ional law. Profili di diritto internazionale pubblico della rete* (Cacucci 2012); and more recently G Della Morte, *Big data e protezione internazionale dei diritti umani. Regole e conflitti* (Editoriale Scientifica 2018) particularly pt I, ch 2.

[61] See Mishra (n 2) 16.

[62] See Sofaer, Clark, Diffie (n 11) 190, noting that although 'current, privately and professionally controlled process for reaching common technology positions on cyber activities is valuable and worth preserving, a mechanism whereby national governments could concur in such positions through an international structure could serve to achieve faster and more uniform acceptance, resulting in more secure and robust cyber networks', also because 'an international arrangement could serve to resolve some if not all the current political manoeuvring over what agencies, states, or other entities should perform key transnational roles in ICT development and security'.

traits that standardization bodies should have to the effect of being recognized under TBT.[63]

As we have seen, digital standards are by their very nature developed in a balkanized context, with a strong influence by private subjects. This feature of digital standardization, with particular reference to cybersecurity, may raise some particular difficulties in ascertaining or acknowledging them for the purpose of TBT.

6. *Conclusion*

Information and communication technologies are today woven into every facet of human activity, from operating nuclear arsenals to raising cows.[64] The postulate for a smooth functioning of ICT are the principles of interoperability and openness.

At the same time, however, there can be no smooth functioning of ICT without cybersecurity. Society as a whole is increasingly dependent on cyber systems across the full range of human activities, including commerce, finance, health care, energy, entertainment, communications, and national defense.[65] It seems therefore reasonable to hold that the need to ensure cybersecurity at the national level may be qualified as a matter of national policy pursuant to the protection of a national interest: cybersecurity's breaches may indeed hamper not only economic interests but also public health and plenty of activities connected to national security.

Such a unilateral approach to cybersecurity, though legitimate at least to a certain extent, may not only hamper trade in digital goods and services but also negatively impact interoperability and its role as a postulate of an interconnected world.

States usually declare that unilateral decisions are taken in order to protect national security. Quite often, however, such measures also have

[63] See P Delimatsis 'Global Standard-Setting 2.0: How the WTO Spotlights ISO and Impacts the Transnational Standard-Setting Process' (2018) 28 Duke J Comparative Intl L 273, 282.

[64] See Finnemore, Hollis (n 4) 426.

[65] See Sofaer, Clark, Diffie (n 11) 179.

the effect of boosting the domestic digital sector and, in a broader perspective, they may also have negative effects on international trade in different sectors.[66]

Traditional dissatisfaction for the lack of international rules aimed at and capable of striking a balance between the potentially clashing interests of global trade, on the one hand, and national rules aiming at ensuring cybersecurity, on the other hand, mainly arose because the WTO agreements (including GATS and TRIPS) are largely considered inadequate to deal with the manifold and complex issues arising from the modern-day digital economy, if only due to the fact that they were adopted more than twenty years ago.[67] It is also certainly true that the WTO, being a trade institution, is not the best placed body to deal with several aspects of digital trade, such as setting standards on cybersecurity or data protection.[68] This inevitably leads to some difficulties in dealing with cybersecurity issues, and to a revived temptation of unilateralism.[69]

As it is hard to imagine that States will soon find a sufficiently shared understanding on these issues, an international agreement on cybersecurity is still far from being a concrete prospect. Therefore, a possible response to a unilateral approach to cybersecurity seems to rely on the interaction between international standardization and the existing WTO legal framework, which could try to reaffirm its centrality with particular reference to digital trade issues. In particular the practice within the TBT

[66] For further references see Mishra (n 2) 5.

[67] With specific regard to the TRIPS Agreement, it has been noted that 'any effective international legal remedy to commercial cyber espionage needs to creatively interpret and apply the terms of TRIPS' (see Malawer (n 15) 158).

[68] The same applies to other relevant aspects such as the determination of the legitimacy of online censorship. On this point see AD Mitchell, N Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy' (2018) 20 Vanderbilt J Entertainment & Technology L 1073, 1122.

[69] The complexity of balancing unilateral approach and the use of international standards in the context of cybersecurity measures are demonstrated by the current debate in the TBT Committee on China's recently enacted cybersecurity law, that has been mentioned above. No wonder that various countries, including in the EU, are raising a number of concerns about China's disregard for international standards, also recalling the risk of a lack of interoperability produced by incompatibilities between national and international standards. See *Statement of the European Union to the Committee on Technical Barriers to Trade*, Doc G/TBT/W/509 (19 April 2018). Similar concerns have also been raised by Japan in relation to Vietnam's draft cybersecurity law. See Committee on Technical Barriers to Trade, *Minutes of the Meeting of 8-9 November 2017*, Doc G/TBT/M/73 (6 March 2018) 2.

Committee shows that WTO law could still be the proper framework in which States may seek harmonization of technical standards related to cybersecurity issues.[70]

This could be a viable solution provided that three conditions are met.

First, this will be possible on the assumption that international standardization in this domain follows some basic principles consolidated in TBT Committee practice since the year 2000, namely transparency, openness, impartiality and consensus, effectiveness and relevance, and respect of the development dimension.

The development of international trade law also in relation to digital technical regulation could then follow the evolutionary approach taken by the DSB in the case of applicability of the GATS to e-commerce services.[71]

Second, a shift should take place in the interpretation of the role of standardization in the digital market. More precisely a truly international perspective on cybersecurity standards requires the understanding that cybersecurity is depending less on aspects such as *where* a given product is produced or by *who* such product is manufactured, than on the different issue of *how* such product is actually made. This clearly entails a far greater importance for technical standards, which may not only ensure technical compatibility about devices produced and operated around the world but also become a viable alternative to most restrictive measures which could potentially be adopted to prevent their trade in order to safeguard cybersecurity.[72]

Third, the principle of technological neutrality should be applied in its full dimension as an interpretive tool for the whole system.

[70] It is probably early to evaluate the full suitability of TBT law in addressing harmonization of cybersecurity technical regulations. Much will depend on whether Member States will be able to find a compromise between the inherent national dimension of cybersecurity measures and the need for a continuous development of common digital standards guaranteeing interoperability and openness of networks, and a fair balance of the interests involved, that also comprise the protection of trade secrets and IPR. The development of international trade law also in relation to digital technical regulation could then follow the evolutionary approach taken by the DSB in the case of applicability of the GATS to e-commerce services.

[71] See S Peng, 'Regulating New Services through Litigation? Electronic Commerce as a Case Study on the Evaluation of "Judicial Activism" in the WTO' (2014) 48 J World Trade 1189.

[72] See Peng, 'Cybersecurity Threats and the WTO' (n 14) 475.

Generally, technological neutrality is a principle of good regulation in Internet, telecommunications and data protection regulation originally established in the context of the International Telecommunication Union. The principle can have various and distinct meanings.[73] The most common understanding of it is that the same regulatory principles should apply regardless of the technology used and therefore regulations should not be drafted in technological silos. Consequently, regulators should adopt, as far as possible, a technologically neutral position. So far, this has been the most common meaning and the one that has been suggested for incorporation in the law of WTO.[74]

Going a step further, the principle can be read as meaning that regulators should refrain from using regulations as a means to push the market toward a particular structure that the regulators consider optimal. In a highly dynamic market, regulators should not try to pick technological winners. In particular, this meaning of the principle of technological neutrality may have a remarkable expanding power and could become the interpretive light for the activity of incorporating digital standards, particularly in the field of cybersecurity, in the framework of WTO law: a useful interpretive tool for the selection and application of standards, which could play a pivotal role in balancing the various interests, both of public and private nature, which are involved in the fragmented and complex process of digital standard setting and regulation.[75]

In conclusion, the battle for smoothly incorporating cybersecurity issues into international trade law is not easy, but it can be won through a truly international standardization capable of keeping cybersecurity needs and openness and interoperability requirements together, under the same umbrella of technological neutrality.

[73] See W Maxwell, M Bourreau 'Technology Neutrality in Internet, Telecoms and Data Protection Regulation' [2015] Computer and Telecommunications L Rev 21

[74] See SY Peng, 'Renegotiate the WTO Schedules of Commitments: Technological Development and Treaty Interpretation' (2012) 45 Cornell Intl L J 403, 427.

[75] Indeed, '[c]yberspace already has a robust and diverse array of norms. National regulations, international laws, professional standards, political agreements, and technical protocols litter the cybersecurity terrain, all involving substantial normative commitments in various stages of development and diffusion' (Finnemore, Hollis (n 4) 427).