Contribution for information to WGEC

Trends and Information for Consideration in the Context of Enhanced Cooperation

Richard Hill[1], October 2017

We present here, for information only, trends and information that appear relevant to us in the context of enhanced cooperation. This paper does not propose any recommendations for consideration by the Working Group on Enhanced Cooperation. This paper is structured as follows:

1. New trends in telecommunications/ICT identified by the Internet Society (ISOC), including information on technology and services
2. A specific trend new trend and the proposed Digital Geneva Convention
3. International legal obligations agreed or proposed in trade negotiations
4. Actual changes in the scope of certain domestic regulatory regimes

1. New trends identified by ISOC

In its 2017 "Global Internet Report: Paths to Our Digital Future"[2], the Internet Society identified a number of trends. We cite here those that appear to us to be relevant in the context of enhanced cooperation (the numbering and structuring below is not in the cited report):

1. The rise of nationalism is challenging our basic notions of global interconnectedness and threatens to fragment the global Internet. (Page 9 of the cited report)
    a. We cannot afford to let the 'securitisation' of the Internet, and our digital lives, run rampant: there is a very real threat that online freedoms and global connectivity will take a back seat to national security. Given the growing pressure from cyber threats and security challenges such as terrorism, the ease with which our open societies and our freedoms and rights could become subordinate to pervasive surveillance regimes facilitated by AI and IoT should not to be underestimated. (Page 10)
    b. Without appropriate safeguards and deliberate efforts to ensure transparency and user control, IoT could drive data collection and use in ways that further undermine privacy. (Page 10)
    c. If governments persist in trying to prevent the use of encryption, they put at risk not only freedom of expression, privacy, and user trust, but the future Internet economy as well. Further, interfering with or weakening encryption technologies will create new vulnerabilities and cyber threats. (Page 39)
2. Addressing cyber threats should be the priority — it is critical for individual safety and for the future Internet economy. (Page 9)
    a. While new Internet-based technologies like the Internet of Things promises economic and social opportunity, their deployment is introducing cybersecurity challenges across all sectors of the economy. Because the ICT sector is no longer isolated, threats to the communications infrastructure are now threats to the entire economy. Developing

[1] http://www.apig.ch

[2] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

countries that are already behind when it comes to cybersecurity readiness will find themselves struggling to keep up with the pace of changing security threats. (Page 81)

b. As the digital network becomes intertwined with everything from lights bulbs to health care to cars, users are increasingly vulnerable to cyberattacks. Today's narrow approach to critical infrastructure protection will be ineffective in a hyperconnected society and economy where all digital infrastructure will be critical. (Page 57)
c. Ultimately, the power of the Internet hinges on users' willingness to trust it. They must trust that their data is secure, that their interactions will be respected, and that their expectations of privacy will be met, among other things. Unfortunately, current trends tell us that trust in the Internet is on the decline, in large measure due to the rising numbers and types of cyber threats and concerns about fake news and disinformation. (Page 72)
d. The lack of clear security and privacy standards for the Internet of Things raises the prospect of a "digital environmental disaster" — a scenario in which abuse of connected objects by criminals, terrorists or even governments escalates to the point that the IoT environment becomes a polluted space in the eyes of consumers. (Page 73)
e. Increased security threats and device vulnerabilities, as well as incompatible standards and a lack of interoperable systems, could well undermine the technology's [IoT's] promise. (Page 10)
f. For IoT to thrive, the security of connected devices must be addressed. (Page 43)
g. A lack of agreement on IoT Security frameworks and best practices may jeopardise the safety of individuals around the globe. (Page 46)
h. The scale of cyberattacks is steadily growing, and many anticipate the likelihood of catastrophic cyberattacks in the future. We already see attacks on a national scale, so it is not farfetched to imagine a digital pandemic with attacks crippling entire economies. As one North American industry analyst put it, a "digital Pearl Harbor is coming …". (Page 56)
i. Governments will face mounting pressure to act forcefully to protect national security, their citizens and their domestic economies. (Page 38)
j. Cyberspace is now considered the fifth domain of warfare, but there are few agreed rules of engagement. The threat of destructive cyber conflict will only increase over the next decade. Conflicts will be initiated not only by nation states, but also by their surrogates, and by independent political movements and private actors. (Page 56)
k. Users must be able to trust that the government agencies and businesses collecting and using their data are resilient and will address cybersecurity threats adequately. (Page 57)

3. New thinking, new approaches and new models are needed across the board, from Internet policy to addressing digital divides, from security approaches to economic regulation. (Page 9)
    a. It is far from clear whether this technology-driven disruption [the Internet economy] will favour the existing Internet platforms or bring greater competition and entrepreneurship. (Page 11)
    b. The ability of new players to emerge could be limited if the trend toward the consolidation of networks under the control of a few large, global players continues. Large Internet platforms are deepening their market positions, dominating Internet infrastructure, services and applications. Smaller networks will simply be unable to compete with large, global

companies that are able to offer services cheaper and make investments into the development of new products and infrastructure development. (Page 84)

c. A small number of major companies may further concentrate their power by absorbing potential threats or new opportunities. The reach and resources of Internet platforms mean that startups will be acquired in their infancy, before they can disrupt the bigger players. (Page 29) [However, the contrary may be the case. (Page 30)]
d. Market consolidation by Internet service and access providers could spur the growth of so-called "walled gardens" — closed platforms with proprietary ecosystems — leading to a loss of choice, constraints on innovation and Internet fragmentation. (Page 25)
e. Developers are increasingly relying on proprietary standards which will be a barrier to innovation and interoperability. (Page 11)
f. Increasingly, developers are relying on proprietary standards which will be a barrier to innovation and interoperability. Open standards development will need to evolve to ensure standards are still relevant in a world of competing proprietary systems. (Page 49)
g. [The] "general purpose" Internet is facing three growing pressures: ubiquitous connectivity; significant changes at the edge of the network (including the devices and applications that generate and use traffic); and the decline of traffic that is passed between backbone networks operated by different entities. (Page 49)
h. [The evolving edge of specialised networks and purpose built services] may create independent islands of connectivity. This could lead to fragmentation of the open, global Internet. If specialised networks dominate the connectivity environment, this will create obstacles for innovation and the deployment of new services and technologies. (Pages 51-52)
i. The nature of transit will change due to the increasing use of Content Delivery Networks (CDNs), caching and other specialised services that flatten the network hierarchy. This may lead to reduced competition and lack of innovation in the core of the network. (Page 49)
j. With increasing international data flows, services and goods will come a need to agree on international norms. (Page 70)
k. Some users already worry about the vast amounts of their personal data being collected and feel powerless to protect their personal privacy. Already, systems use data profiling to draw inferences about individual beliefs, preferences or habits in ways that are deeply personal. (Page 76)
l. Without investments in core infrastructure to support the growth in connected devices, citizens will be unable to benefit fully from the digital economy. (Page 83)

4. Multistakeholder approaches to Internet policy will become ever more relevant in a world in which the physical and the digital worlds converge and as the cross-border nature of Internet challenges becomes clear. (Page 9)
    a. From cybersecurity to societal issues to technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), governments will face a host of new and complex issues that will challenge all aspects of their decision-making. (Page 37)

b. Governments may turn to multi-stakeholder models of policy development out of necessity, as traditional telecommunications and Internet regulatory approaches are longer seen as fit for purpose. (Page 40)

2. The trend leading to calls for a Digital Geneva Convention

As noted above, threats to the communications infrastructure are now threats to the entire economy. As the digital network becomes intertwined with everything from lights bulbs to health care to cars, users are increasingly vulnerable to cyberattacks. The scale of cyberattacks is steadily growing, and many anticipate the likelihood of catastrophic cyberattacks in the future. Cyberspace is now considered the fifth domain of warfare, but there are few agreed rules of engagement. The threat of destructive cyber conflict will only increase over the next decade. Conflicts will be initiated not only by nation states, but also by their surrogates, and by independent political movements and private actors.

The 22 July 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[3] (document A/70/174) includes in its paragraph 13 the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

> (a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
>
> (f) A State should not conduct or knowingly support ICT activity contrary to its 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;
>
> (i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
>
> (j) States should 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;

In our view, the proposed norms are relevant in the context of the review of the ITRs. For greater detail, please refer to APIG's Comments on Open Consultation on UN GGE 2015 Norm Proposals, available at:

http://www.apig.ch/GGE%202015%20norm%20comments.pdf

[3] https://undocs.org/A/70/174

Further, as stated by the President of a leading software company (Microsoft)[4]:

> 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.
>
> In short, the time has come for governments to adopt a Digital Geneva Convention to protect civilians on the internet.
>
> …
>
> … governments around the world should pursue a broader multilateral agreement that affirms recent cybersecurity norms as global rules. Just as the world's governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, we need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace.
>
> Such a convention should commit governments to avoiding cyber-attacks 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.
>
> In addition, a Digital Geneva Convention needs to create an independent organization that spans the public and private sectors. Specifically, the world needs an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries.
>
> While there is no perfect analogy, the world needs an organization that can address cyber threats in a manner like the role played by the International Atomic Energy Agency in the field of nuclear non-proliferation. This organization should consist of technical experts from across governments, the private sector, academia and civil society with the capability to examine specific attacks and share the evidence showing that a given attack was by a specific nation-state. Only then will nation-states know that if they violate the rules, the world will learn about it.

[4] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4

In a press conference on 11 May 2017[5], the official presenting the cited US Executive Order[6] stated:

> ... I think the [security] trend is going in the wrong direction in cyberspace, and it's time to stop that trend ... . We've seen increasing attacks from allies, adversaries, primarily nation states but also non-nation state actors, and sitting by and doing nothing is no longer an option.
>
> ...
>
> ... [several] nation states are motivated to use cyber capacity and cyber tools to attack our people and our governments and their data. And that's something that we can no longer abide. We need to establish the rules of the road for proper behavior on the Internet, but we also then need to deter those who don't want to abide by those rules.

Following the WannaCrypt attack[7] in mid-May 2017, Microsoft reinforced its call for action, stating[8]:

> Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.
>
> The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.

Civil society organizations have also called for treaty provisions to ensure that the Internet is used only for peaceful purposes.[9]

---

[5] https://www.whitehouse.gov/the-press-office/2017/05/11/press-briefing-principal-deputy-press-secretary-sarah-sanders-and

[6] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, available at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[7] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

[8] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00017arazqit2faipqq2lyngzmxx4 ; see also: https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/

3. International legal obligations agreed or proposed in trade negotiations

Numerous provisions agreed in the TransPacific Partnership (TPP) treaty create new international legal obligations[10]. Similar provisions have been proposed for the Trade in Services Agreement (TiSA)[11] and related provisions have been proposed for discussion and/or negotiation in the World Trade Organization (WTO)[12]. Violations of provisions of WTO agreements are subject to review in a formal dispute settlement system, under which compensating remedies[13] can be ordered; however, it should be noted that some states have criticized[14] certain aspects of the WTO dispute settlement system.

Some of the provisions in question are related to the mandate of the ITU. As information regarding areas where cooperation could be enhanced, we outline below the relevant areas of ITU work and the provisions in question.

3.1 Allocation and use of frequencies and numbers

ITU: numerous Recommendations, Resolutions and even treaty provisions for frequencies.

WTO: specific provisions in TISA, TPP, including number portability in TPP.

3.2 Access to infrastructure and interconnection

ITU: best practices and capacity building for conditions for the use of infrastructure by competitors and for interconnection.

WTO: specific provisions in TISA, TPP, including co-location in TPP. Proposals in WTO for its e-commerce agenda.

3.3 Internet Interconnection

ITU: Recommendations.

WTO: TPP E-Commerce Chapter, art. 14.12 states "The Parties recognise that a supplier seeking international Internet connection should be able to negotiate with suppliers of another Party on a

---

[9] See point 5 of the Delhi Declaration, at https://justnetcoalition.org/delhi-declaration ; see also http://twn.my/title2/resurgence/2017/319-320/cover08.htm

[10] See the Telecommunication and E-Commerce chapters of the treaty, available at: https://www.mfat.govt.nz/en/about-us/who-we-are/treaties/trans-pacific-partnership-agreement-tpp/text-of-the-trans-pacific-partnership

[11] See http://www.uniglobalunion.org/news/tisa-foul-play

[12] See https://dig.watch/sessions/making-trade-more-inclusive-through-digitally-enabled-services https://www.twn.my/title2/wto.info/2017/ti170917.htm https://www.newsclick.in/e-commerce-discussions-wto-more-neo-liberal-policies-negotiated-secret

[13] For an example, see: https://www.ip-watch.org/2017/09/29/us-misrepresentations-called-antigua-online-gambling-case/

[14] https://www.csis.org/analysis/us-trade-policy-priorities-robert-lighthizer-united-states-trade-representative https://www.ft.com/content/3459f930-a532-11e7-9e4f-7f5e6a7c98a2

commercial basis. These negotiations may include negotiations regarding compensation for the establishment, operation and maintenance of facilities of the respective suppliers."

3.4 Security

ITU: numerous Recommendations, treaty provisions.

WTO: TPP E-Commerce Chapter art. 14.15 and 14.16 call for cooperation regarding security and cybersecurity. Proposals in WTO for its e-commerce agenda.

3.5 Spam

ITU: numerous Recommendations, treaty provisions.

WTO: TPP E-Commerce Chapter art. 14.14. Art. 14.15 calls for cooperation regarding spam. Proposals in WTO for its e-commerce agenda.

3.6 Open Source

ITU: Resolution.

WTO: TPP E-Commerce Chapter art. 14.17 restricts use of open source.

3.7 Universal service

ITU: best practices and capacity building.

WTO: specific provisions in TISA, TPP.

3.8 Roaming

ITU: Recommendations and treaty provisions.

WTO: specific provisions in TISA, TPP.

3.9 Regulatory body and licensing

ITU: best practices and capacity building for independent regulatory authority and licensing.

WTO: specific provisions in TISA, TPP. Proposals in WTO for its e-commerce agenda.

3.10 Recourse

Telecom operators have right to have recourse to the regulatory and competition authorities of other states.

ITU: proposed for the 2012 ITRs, rejected by some Member States.

WTO: present in TISA, TPP.

4. Actual changes in the scope of certain domestic regulatory regimes

Several countries[15], in particular Brazil, Chile, the European Union, India, and the USA have imposed network neutrality regulations[16].

In February 2015, the United States Federal Communication Commission (FCC) adopted an order[17] in which it reclassified certain Internet services so that they would be subject to certain provisions of the US telecommunication regulations. In essence, the FCC reclassified broadband Internet access services and imposed network neutrality provisions. Subsequently, the FCC initiated a process to reverse that order. In the context of that process, a group of Internet technologists has submitted a comment[18] to the FCC in which they explain how the Internet has evolved, and, given that evolution, why certain aspects of the Internet (in particular access) are functionally similar to certain aspects of the telephone network and thus should be regulated (or not) in similar ways.

_____

[15] See https://en.wikipedia.org/wiki/Net_neutrality_law

[16] A comparison of the approaches taken in Chile, India, and the USA is provided in: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/7243-study-on-net-neutrality-regulation_0.pdf

[17] https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

[18] https://www.eff.org/files/2017/07/17/comments_of_internet_engineersfcc_nn.pdf