Comments on
Promoting Stakeholder Action Against Botnets and Other Automated Threats

Richard Hill, Association for Proper Internet Governance[1]

January 2018

This paper contains our comments on the draft report at:

https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

The call for comments is at:

https://www.ntia.doc.gov/federal-register-notice/2018/rfc-promoting-stakeholder-action-against-botnets-other-automated-threats

We endorse and support the analysis and recommendations in the draft report. Regarding Action 4.2, promoting international adoption of best practices and relevant tools through bilateral and multilateral international engagement efforts, we would suggest the following additional specific actions.

1. Promote adoption and implementation of the eleven norms of paragraph 13 of the UN GGE 2015 report

We refer to the best practice norms presented in 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)[2].

We are of the view that adoption and implementation of those norms should be promoted.

Further, we believe that relevant reference material, that should be considered when implementing the proposed norms, includes the 2012 International Telecommunications Regulations (ITRs)[3], a treaty of the International Telecommunication Union (ITU)[4], and the following scholarly comments[5] on that instrument:

- Hill, Richard (2013), "WCIT: failure or success, impasse or way forward?", *International Journal of Law and Information Technology,* vol. 21 no. 3, p. 313, DOI:10.1093/ijlit/eat008
- Hill, Richard (2013), *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History,* Schulthess/Springer

We list each of the proposed norms and then comment as to how to best understand and implement it.

(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;

The proposed norm is, in our view, relevant and justified.

---

[1] info@apig.ch

[2] https://daccess-ods.un.org/access.nsf/GetFile?Open&DS=A/70/174&Lang=E&Type=DOC

[3] http://www.itu.int/en/wcit-12/Pages/default.aspx

[4] http://www.itu.int/en/Pages/default.aspx

[5] For more information, see: http://www.hill-a.ch/wcit

Article 6 of the ITRs states:

> Member States shall individually and collectively endeavour 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.

This treaty provision would appear to implement the proposed norm. Consequently, it is suggested that all states should agree to be bound by this article of the ITRs.[6]

In order to more closely align with the proposed norm, article 6 of the ITRs could be modified to read as follows:

> Member States shall endeavour[7], individually and in cooperation, to 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.

(b) In case of ICT incidents, States should 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;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing an additional provision for article 6 of the ITRs, for example:

> In case of ICT incidents, Member States shall endeavor to 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.

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing an additional provision for article 6 of the ITRs, for example:

---

[6] A number of states refused to sign the ITRs in 2012. The reasons given, in particular that article 6 might justify violations of freedom of speech, are not valid from a legal point of view, see the cited scholarly works. For greater clarity, states acceding to the ITRs could make a formal declaration along the lines of the proposal at:
http://www.hill-a.ch/ITR%20accession.doc

[7] During the negotiations of the ITRs, the point was made that it might be impossible for a state to ensure certain aspects of cybersecurity, so the use of the term "shall" did not achieve consensus. On the other hand, it point was made that the term "should" is too weak. As a compromise, it was agreed to use the term "shall endeavor", which means that states must make efforts to implement the provision. See the discussion on pp. 95-96 of Hill, Richard (2013), *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History,* Schulthess/Springer.

> Member States shall endeavour not knowingly to allow their territory to be used for internationally wrongful acts using ICTs.

(d) States should 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. States may need to consider whether new measures need to be developed in this respect;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing an additional provision for article 6 of the ITRs, for example:

> Member States shall endeavor to 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.

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

The proposed norm is, in our view, relevant and justified.

This norm is covered by the Preamble of the ITRs, which states:

> Member States affirm their commitment to implement these Regulations in a manner that respects and upholds their human rights obligations.

(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;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing an additional provision for article 6 of the ITRs, for example:

> Member States shall endeavor not to 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.

(g) States should 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;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing an additional provision for article 6 of the ITRs, for example:

> Member States shall endeavor to 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.

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should 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;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing a additional provisions for article 6 of the ITRs, for example:

> Member States shall endeavor to respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.
>
> Member States shall also endeavor to 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.

(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;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing additional provisions for article 6 of the ITRs, for example:

> Member States shall endeavor to take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.
>
> Member States shall endeavor 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;

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing an additional provision for article 6 of the ITRs, for example:

> Member States shall endeavor to 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.

(k) States should 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 State should not use authorized emergency response teams to engage in malicious international activity.

The proposed norm is, in our view, relevant and justified.

This norm could be implemented by agreeing additional provisions for article 6 of the ITRs, for example:

> Member States shall endeavor not to 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 Member State shall endeavor not to use authorized emergency response teams to engage in malicious international activity

2. Additional recommendations

A well-know software company has recently called for steps to be taken to address the very real cyber-security threats that the world is facing.[8]

Those proposals[9] are, in our view, relevant and justified.

The proposals regarding a Digital Convention and an Attribution Organization could be implemented by agreeing additional provisions for the ITRs. Some of the proposals in question are covered by the proposals in section 1 above. The following additional proposals could be considered:

Member States shall endeavor to refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes.

Member States shall endeavor to refrain from using ICTs to steal the intellectual property of private companies, including trade secrets or other confidential business information, to provide competitive advantage to other companies or commercial sectors.

Member States shall endeavor to refrain from inserting or requiring "backdoors" in mass-market commercial technology products.

Member States shall endeavor to 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.

Member States shall endeavor to exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise, and not reusable; Member States shall also endeavor to also ensure that they maintain control of their weapons in a secure environment.

Member States shall endeavor to 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.

Member States shall endeavor to limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.

Member States shall endeavor to assist private sector efforts to detect, contain, respond, and recover in the face of cyberattacks; in particular, 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.

---

[8] See https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4
https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/

[9] The proposals were published in June 2017 at the following web sites, but are no longer available there:
https://mscorpmedia.azureedge.net/mscorpmedia/2017/04/Policy-Paper-Digital-Geneva-Convention.pdf
https://mscorpmedia.azureedge.net/mscorpmedia/2017/04/Policy-Paper-Attribution-Organization.pdf
https://mscorpmedia.azureedge.net/mscorpmedia/2017/04/Policy-Paper-Industry-Accord.pdf

Member States shall endeavor to facilitate the establishment of an international cyberattack attribution organization to strengthen trust online.

That organization shall be independent of Member States; it could be modelled on the International Federation of Red Cross and Red Crescent Societies; its membership could consist of CERTs.[10]

_____

[10] This proposal is not part of Microsoft's proposal. It is a proposal by the author of this submission.