ICT for peace foundation

CYBER SECURITY POLICY PROCESS

BRIEF

TRUST AND ATTRIBUTION IN CYBERSPACE:

A PROPOSAL FOR AN INDEPENDENT NETWORK OF ORGANISATIONS ENGAGING IN ATTRIBUTION PEER-REVIEW

Serge Droz & Daniel Stauffacher

GENEVA 2018
ICT4Peace Foundation

ICT4Peace Publishing, Geneva. 2018
Copies available from www.ict4peace.org

TRUST AND ATTRIBUTION IN CYBERSPACE:

A PROPOSAL FOR AN INDEPENDENT NETWORK OF ORGANISATIONS ENGAGING IN ATTRIBUTION PEER-REVIEW

Serge Droz & Daniel Stauffacher

ICT for peace foundation

ABSTRACT

Most nations share the view that existing international legal rules and ordinances hold in cyberspace. Enforcement of these standards, however, is difficult. Malicious cyber activities are usually shrouded in secrecy and anonymity, making definite attribution difficult and even impossible at times.

This brief thought piece takes into account the technical and political challenges related to effective attribution, and presents a simple proposal for improvement, namely the setting up of an independent network of organisations engaging in attribution peer-review.

TRUST AND ATTRIBUTION IN CYBERSPACE:

A PROPOSAL FOR AN INDEPENDENT NETWORK OF ORGANISATIONS ENGAGING IN ATTRIBUTION PEER-REVIEW

International Law in Cyberspace

Both the 2013 and the 2015 editions of the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security declared that "international law, and in particular the Charter of the United Nations" is applicable to cyberspace.[1] In spite of this, cyberspace presents a domain in which the actions of unscrupulous governments and malevolent private perpetrators often go unpunished.

There are few formal international legal agreements that provide clear guidance and regulate how nations ought to contain cybercrime, for example. One exception is the Budapest Convention, which seeks to "pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation".[2] While laudable and ambitious in its goals, the convention lacks critical endorsement of major cyber powers, including Russia and China. Among other things, the latter object to the convention's provision for authorised access to information infrastructure in another state's jurisdiction.[3]

1 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 2015, para. 24, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

2 Council of Europe, "Convention on Cybercrime" (2001), sec. Preamble, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

3 Keir Giles, "Russia's Public Stance on Cyberspace Issues," in IEEE Xplore (IEEE, 2012), http://ieeexplore.ieee.org/document/6243966/.

In terms of legal guidance efforts, the Tallinn Manuals (1 and 2) also deserve mention.[4] Although developed without the official participation of government representatives and merely advisory in nature, the Tallinn Manuals present one of the most comprehensive treatises on the applicability of international law to the virtual realm to date.[5]

Owing to deep-running ideological differences and political stand-offs, today's political climate does not seem conductive to the conclusion of new international treaties. As a result, and instead of binding legal instruments, softer measures such as voluntary norms for responsible (state) behaviour in cyberspace and confidence building measures (CBMs) have been proposed to increase the stability and security of the virtual domain.[6]

Attribution

For laws and norms to be effective in regulating conduct in cyberspace, violations of the former must be detected, and perpetrations attributed beyond reasonable doubt. The process of assigning blame for cyber attacks requires intricate political and technical forensics and skills, "weaving together [...] clues concerning past attack methods, current operational techniques, and knowledge of adversaries' geopolitical objectives to identify a likely [culprit]".[7]

4 Michael N. Schmitt, "Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't," 2017, accessed March 28, 2018, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/; Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, ed. Michael N. Schmitt (Cambridge: Cambridge University Press, 2013), https://doi.org/10.1017/CBO9781139169288.

5 Michael J. Adams and Megan Reiss, "International Law and Cyberspace: Evolving Views," Lawfare, 2018, https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views.

6 OSCE, "OSCE Confidence-Building Measures to Reduce the Riss of Conflict Stemming from the Use of Information and Communication Technologies," 2016, https://www.osce.org/pc/227281?download=true; United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security."

7 William G. Rich, "The US Leans on Private Firms to Expose Foreign Hackers," WIRED, 2018, https://www.wired.com/story/private-firms-do-government-dirty-work/?mbid=social_twitter&utm_brand=wired&utm_campaign=wired&utm_medium=social&utm_social-type=owned&utm_source=twitter.

With a view to achieving higher levels of confidence vis-a-vis ascribing blame for nefarious behaviour in cyberspace and introducing accountability, some experts have suggested the creation of an international attribution body similar to established enforcement mechanisms such as the International Atomic Energy Authority[8]. There are, however, profound differences between nuclear and information technologies, and the nature of nuclear arms and cyber weapons, respectively.

Nuclear technology is industrial by design. It is difficult, if not impossible, to develop nuclear capabilities in hiding. Also, military use of nuclear technology is very different from civilian use. Cyber capabilities on the other hand are software based. In contrast to nuclear technology, cyber tools do not emit suspicious radiation and do not require factories for their development. A handful of dedicated individuals gathered in a room can launch a cyberattack of sizeable magnitude. Furthermore, military and civilian use of cyber capabilities and relevant infrastructures overlap at times. Governments have been seen to employ cyber means to target civilian

Plea for a Global Cyber Attribution Network

In order to curb adverse effects stemming from the misuse of offensive cyber capabilities, effective, technically mature and above all trustworthy attribution is indispensable. "There are an increasing number of government entities, private firms, and research organisations that have the capability to undertake investigations to attribute the source of cyber attacks. However, these entities do not follow a standardised research methodology and employ different naming conventions for cyber threat actors and confidence metrics for their findings".[9]

With a view to addressing these inconsistencies and contributing to a more secure and stable digital environment, ICT4Peace proposes the setting up of an independent network of organisations engaging in attribution peer-review. For international legal provisions to be effective and accountability for malicious cyber activities to take

8 Microsoft, "An Attribution Organization to Strengthen Trust Online," 2017, https://www.microsoft.com/en-us/cybersecurity/content-hub/an-attribution-organization-to-strengthen-trust-online; Karl Grindal et al., "Is It Time to Institutionalize Cyber Attribution," 2018, https://via.hypothes.is/https://www.internetgovernance.org/wp-content/uploads/WhitePaper-Attribution-23-8.pdf; Jason Healey, John C Mallery, and Nathaniel V Youd, "Confidence-Building Measures in Cyberspace a Multistakeholder Approach for Stability and Security Measures in Cyberspace Stability and Security," 2014, 28.

9 John S. Davis et al., Stateless Attribution: Toward International Accountability in Cyberspace, 2017, 2, http://www.rand.org/pubs/research_reports/RR2081.html.

hold high levels of confidence and publicly persuasive attribution of responsibility are required.[10] In cyberspace, where establishing proof claims beyond reasonable doubt is still challenging, secrecy and mistrust are prevailing, and multiple factors (economic, political, technical) need to be taken into regard, collaborative attribution practices seem most promising.

Building on Deibert's idea of an academic network engaging in global attribution efforts, ICT4Peace's proposal goes one step further and expands the list of possible contributors.[11] The network of independent attribution actors as envisaged by ICT4Peace should include government representatives, private sector pundits as well as proponents from civil society and academia.[12]

In terms of mode d'emploi, following standardised guidelines, the members of the network would operate and conduct relevant analyses independently and later submit their attribution results to a peer-review process. While there may be a coordinating entity engaging with third parties and communicating results, the attribution work per se would be carried out by the individual members of the network. Given the network's multistakeholder setup, criticism related to political or economic bias, limited or opaque evidence, inconsistent evaluation methodologies or lacking legitimacy would be hard to sustain.

Open Issues and Questions

Currently, the majority of attribution efforts is conducted by private threat intelligence organisations and national security agencies. Before a more inclusive global cyber attribution network such as the one envisioned by ICT4Peace can come into effect, a number of critical questions have to be addressed:

- Who are the initial members? Ideally the network would start small with a concrete mission.

10 Davis et al., Stateless Attribution: Toward International Accountability in Cyberspace.

11 Howard Solomon, "RightsCon Report: Universities Should Form Cyber Attribution Network," IT World Canada News, 2018, https://www.itworldcanada.com/article/rightscon-report-universities-should-form-cyber-attribution-network/405399.

12 Camino Kavanagh and Daniel Stauffacher, "A Role for Civil Society in Cybersecurity Affairs," ICT4Peace, 2015, https://ict4peace.org/activities/policy-research/policy-research-cs/first-ict4peace-publication-in-spanish-a-role-for-civil-society-in-cybersecurity-affairs/.

- What is the scope of the mission and what legal institutional logic should the network be based upon (i.e. foundation)?
- How are stakeholders being recruited and integrated? How can diversity be guaranteed and adversarial political relationships be used constructively?
- What are the entry requirements for members of the network? The network should be open to different kinds of organisations interested in attribution. What are relevant codes of conduct and base-line ethics thresholds?
- What will the peer-review process look like and how will it be structured?
- How will confidential information be used in attribution?
- What formats and standards will be used to exchange results? Every published analysis should be replicable by capable third parties, or at least other members of the network.
- How will the network be financed? Should financing be made transparent?
- What are the reporting guidelines and how often should results be reported?
- How will transparency, accountability and responsibility be ensured?
- What decision making procedures would be underlying the network?

Conclusion

Against the background of seemingly ceaselessly proliferating cybersecurity incidents, ICT4Peace is driven to address these questions and work on collaborative solutions to increase the security and stability of cyberspace. Recent normative efforts by state and non-state actors alike have served and continue to serve as important steps towards clearer understandings apropos responsible behaviour in cyberspace.[13] However, "without the ability to know when an attack has occurred and who is behind the effort, the greatest offenders are enabled to flout the international efforts. Thus, the ability to know who is responsible is the linchpin of accountability, [and needs to be further strengthened]."[14] The peer-review-based global cyber attribution network introduced above may help instil trust in forensic evidence and create responsibility.

13 Paul Meyer, "Global Cyber Security Norms: A Proliferation Problem?," ICT4Peace, 2018, https://ict4peace.org/activities/global-cyber-security-norms-a-proliferation-problem/.

14 Davis et al., Stateless Attribution: Toward International Accountability in Cybvverspace, 43.

The authors

Serge Droz

Dr. Serge Droz is the Vice President CERT (Computer Emergency Response Team) at Open Systems, one of the leading managed security service providers in Europe. He studied physics at ETH Zurich and the University of Alberta, Canada and holds a PhD in theoretical astrophysics. Before joining Open Systems, he worked in academia in Switzerland and USA, later as a Chief Security Officer of Paul Scherrer Institute, as well as in different security roles at SWITCH for more than 15 years. Serge is a member of the board of directors of FIRST (Forum for Incident Response and Security Teams), the premier organisation of recognised global leaders in incident response. He also served for 2 years in the ENISA (European Union Agency for Network and Information Security) permanent stakeholder group. Serge is an active speaker and a regular trainer for CSIRT (Computer Security Incident Response Team) courses around the world.

Daniel Stauffacher

A former Ambassador of Switzerland, is a founder and President of the ICT4Peace Foundation, which since 2003 explores, champions the use of Information and Communication Technologies (ICT) for peace-building, crisis management, and humanitarian aid, and supports diplomatic processes for a peaceful and open cyberspace. He has a Master's degree from Columbia University, New York and a Ph.D. in media and copyright law from the University of Zürich. After managing a Swiss publishing company, he joined the United Nations Development Program (UNDP) in 1982 and worked in New York, Laos and China. In 1990 he joined the Swiss Federal Office for Foreign Economic Affairs (Bawi) and in 1995 he was posted to the Swiss Mission to the European Union in Brussels. From 1999 to 2005 he was the Swiss Ambassador and the Swiss Federal Council's Special Representative for the hosting and preparation of the World Summit on Social Development plus 5 in 2000 in Geneva and the UN World Summit on the Information Society (WSIS) which was held in Geneva in 2003 and in Tunis 2005. He was a member of UN SG Kofi Annan's UN ICT Task Force and a Co-Chair of the Global Alliance for ICT for Development (GAID) and a Founder and President of the Geneva Security Forum. He is a founding Trustee of Sir Tim Berners Lee's World Wide Web Foundation.

Since 2007 he served as an advisor to the Swiss, Swedish and other Governments and to the UN Secretariat General and a number of UN organisations on improving the

UN Crisis Information Management Systems (CiMS) for humanitarian, peace-keeping and peace-building operations. He has also been an Advisor to several Governments, the UN, OSCE, OAS, AU, ASEAN on International Cyber Security Policy, Diplomacy and Capacity Building and has co-launched with the UN the Tech Against Terrorism Project. He is the President and Founder of the Zurich Hub for Ethics and Technology (ZHET) He has been invited to speak and moderate discussions at numerous global conferences and published in these emerging fields. He is an Alumni of the Harvard Law School's Berkman Center on Internet and Society and the Geneva Center for Security Policy (GCSP). Dr. Daniel Stauffacher is President of Dr. Daniel Stauffacher + Partner, a consulting firm based in Switzerland that helps build partnerships for innovation among governments, international organisations, civil society and private-sector entities.

References

Adams, Michael J., and Megan Reiss. “International Law and Cyberspace: Evolving Views.” Lawfare, 2018. https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views.

Council of Europe. Convention on Cybercrime (2001). https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

Davis, John S., Benjamin Boudreaux, Jonathan William Welburn, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase. Stateless Attribution: Toward International Accountability in Cyberspace, 2017. http://www.rand.org/pubs/research_reports/RR2081.html.

Giles, Keir. “Russia’s Public Stance on Cyberspace Issues.” In IEEE Xplore. IEEE, 2012. http://ieeexplore.ieee.org/document/6243966/.

Grindal, Karl, Brenden Kuerbis, Farzaneh Badiei, and Milton Mueller. “Is It Time to Institutionalize Cyber Attribution,” 2018. https://via.hypothes.is/ https://www.internetgovernance.org/wp-content/uploads/WhitePaper-Attribution-23-8.pdf.

Healey, Jason, John C Mallery, and Nathaniel V Youd. “Confidence-Building Measures in Cyberspace a Multistakeholder Approach for Stability and Security Measures in Cyberspace Stability and Security,” 2014, 28.

Kavanagh, Camino, and Daniel Stauffacher. “A Role for Civil Society in Cybersecurity Affairs.” ICT4Peace, 2015. https://ict4peace.org/activities/policy-research/policy-research-cs/first-ict4peace-publication-in-spanish-a-role-for-civil-society-in-cybersecurity-affairs/.

Meyer, Paul. “Global Cyber Security Norms: A Proliferation Problem?” ICT4Peace, 2018. https://ict4peace.org/activities/global-cyber-security-norms-a-proliferation-problem/.

Microsoft. “An Attribution Organization to Strengthen Trust Online,” 2017. https://www.microsoft.com/en-us/cybersecurity/content-hub/an-attribution-organization-to-strengthen-trust-online.

OSCE. “OSCE Confidence-Building Measures to Reduce the Riss of Conflict Stemming from the Use of Information and Communication Technologies,” 2016. https://www.osce.org/pc/227281?download=true.

Rich, William G. “The US Leans on Private Firms to Expose Foreign Hackers.” WIRED, 2018. https://www.wired.com/story/private-firms-do-government-dirty-

work/?mbid=social_twitter&utm_brand=wired&utm_campaign=wired&utm_medium=social&utm_social-type=owned&utm_source=twitter.

Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't." 2017. Accessed March 28, 2018. https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/.

———. Tallinn Manual on the International Law Applicable to Cyber Warfare. Edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139169288.

Solomon, Howard. "RightsCon Report: Universities Should Form Cyber Attribution Network." IT World Canada News, 2018. https://www.itworldcanada.com/article/rightscon-report-universities-should-form-cyber-attribution-network/405399.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organisations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with the publication of a book by the UN ICT Task Force on the practice and theory of ICT in the conflict cycle and peace building in 2005 and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation