Closing the accountability gap:
A proposal for an evidence-led accountability framework

CyberPeace Institute Position Paper

Submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'

December 2019

The accountability gap

The growing weaponization of the Internet reflects the current threat landscape, where state and non-state actors are conducting cyber operations with little risk to be held accountable.[1] From hijacking systems and ransomware attacks to cyberespionage attempts, malicious actors deploy cyberweapons to undermine hospitals, telecommunications networks, transportation systems, and critical public services. The current digital age is fraught with problems relating to our rights, and at the core of these issues is the inherent lawlessness of the cyberdomain.

With only a surface view of what is happening, it is almost impossible to fully know what is raging in the cyberspace.[2] However, it is vital to draw the global attention back to the impact of cyberthreats on civilians in order to avoid them from being turned into vulnerable targets.[3] The multiplication and lack of thorough investigations after major attacks leaves people

[1] GCSC, *Final Report: Advancing Cyberstability*, November 2018, https://cyberstability.org/wp-content/uploads/2019/11/Digital-GCSC-Final-Report-Nov-2019_LowRes.pdf.
[2] Edited by Patryk Pawlak and Thomas Biersteker, *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace*, EUISS, Chaillot Paper/155, October 2019, https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf.
[3] See for further reference ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, 2019, https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

desensitized, disillusioned, and disempowered; therefore, crippling their trust in institutions and governments.[4]

Not closing the accountability gap means a widening of the digital divide between who has the capabilities in place to react to cyberattacks, and who does not. More importantly, not addressing and closing the accountability gap will deepen the void between victims and perpetrators.

The CyberPeace Institute strongly urges the Member States to recognize the systemic disruption caused by cyberattacks, which ultimately leads to an erosion of trust in democracy, and in society as a whole. The CyberPeace Institute would like to address this deficit of trust head-on by working to close the accountability gap in cyberspace.

Frameworks for accountability

The current accountability gap lies in the absence of restrictions to the development and trade in digital weapons, and absence of incentives for responsible behaviour as a means to de-escalate cyber operations.[5] Insofar, one effective framework to address the issue of accountability is to enact globally recognized norms and regulations. However, this type of top-down construct is challenged by the very nature of the cyberspace, as it is inherently entangled with transnational supply chains, the abundance of interconnected technologies and the convergence of disruptive digital services. These are not easily governed by any international legal construct. As a matter of fact, neither norms nor regulations constitute law in the cyberspace nowadays. In a space which is an organic construct of hardware, networks and software, the code and the protocols have become informal laws as they frame the understanding of the threats and the rules of engagement about how to react. Therefore, an additional framework for accountability needs to be built whilst taking the technical construct of the cyberspace into consideration.[6] Finally, the impact of cyberattacks is expressed as a cost to infrastructure or business disruption; we need to bring the human dimension of the attack and the rights of civilians back at the core. **There can't be any framework for accountability if the victims are not at the centre of the discussions**.

The CyberPeace Institute calls the UN GGE and the UN OEWG to address the accountability gap through multiple facets: a top down approach for the international community to design an overarching framework, and a bottom-up approach where grassroots practitioners propose actionable accountability measures on the basis of the technical reality of the cyberspace and the human cost of cyberattacks.

---

[4] Marietje Schaake, *Closing the Accountability Gap for Harms in Cyberspace*, CyberPeace Institute, 2019, https://cyberpeaceinstitute.org/latest-insights/2019-11-08-closing-the-accountability-gap-for-harms-in-cyberspace.

[5] See for further reference Angela McKay et al., *International Cybersecurity Norms: reducing conflict in an Internet-dependent world*, Microsoft, 2014, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA.

[6] GCSC, *Final Report: Advancing Cyberstability*, November 2018, https://cyberstability.org/wp-content/uploads/2019/11/Digital-GCSC-Final-Report-Nov-2019_LowRes.pdf.

The CyberPeace Institute would also call on these groups to consider a governance model to enforce accountability frameworks. The accountability gap is perpetrated by the fact that there is no final arbiter in cyberspace governance.[7] Who would hold who accountable, and who has the legitimacy to do so?

Evidence-led accountability and capacity-building

As a first step to address the complex issue of accountability, the CyberPeace Institute proposes to coordinate a multi-stakeholder response through collective analysis of major attacks. The CyberPeace Institute considers negating malicious actors with the possibility of acting covertly in the cyberspace a collective responsibility. In that regard, the CyberPeace Institute salutes ICT4Peace's initiative for an independent, peer-review network for the purpose of attribution.[8] The CyberPeace Institute aims to coordinate analysis, conducted by the highest forensic standards, and inclusive of public/private international cyber expertise.

Our aim is to deliver actionable insights to the public, with a focus on the victims of cyberattacks. The cyberspace is a common good, and how malicious actors are abusing it should be public knowledge. The CyberPeace Institute will focus on tangible issues **and wishes to help build an actionable and evidence-led accountability framework**. With this in mind, our aim is to inform the UN GGE and the UN OEWG discussions on norms and regulations, as this should facilitate the adoption of voluntary standards, behaviours and code of conducts. Specifically, this analysis will support the design of capacity-building tools and methodologies for vulnerable communities. It is our hope that this analysis will support the work of grassroots practitioners who are already servicing these communities. **Closing the accountability gap will also happen by delivering scalable and sustainable solutions to vulnerable communities targeted by major attacks.**

This paper works to emphasize that the CyberPeace Institute believes that civilians need to be brought back to the forefront in cybersecurity discussions and be empowered in understanding how their infrastructures are attacked. Through collective analysis of cyberattacks and capacity-building measures grounded in internationally accepted norms, the CyberPeace Institute is confident that positive changes will be made towards the protection of civilians and the overall stability in cyberspace. We commend the OEWG's inclusive approach towards civil society, academia and the private sector, and the CyberPeace Institute will continue contributing to its work.

Stéphane Duguin
Geneva, 01/12/2019

[7] Jacqueline Eggenschwiler, *Accountability Challenges confronting Cyberspace Governance*, Journal on Internet Regulation, vol. 6, no. 3, 2017, https://policyreview.info/node/712/pdf.
[8] Serge Droz and Daniel Stauffacher, *Trust and Attribution in Cyberspace: A Proposal for an Independent Network of Organizations engaging in Attribution Peer-Review*, ICT4Peace Foundation, 2018, https://ict4peace.org/wp-content/uploads/2019/07/ICT4Peace-2019-Trust-and-Attribution-in-Cyberspace.pdf.