Memorandum on Microsoft's Proposed Digital Geneva Convention

May 4, 2023

Joseph Zuccarelli

MEMORANDUM FOR IGA 236 (CYBERSECURITY: TECHNOLOGY, POLICY, AND LAW) TEACHING STAFF

Section 1. Introduction. Governments across the world are investing more resources than ever in the development of offensive cyber capabilities. As a result, nation-state cyber-attacks are becoming increasingly common, prompting the need for a set of international rules to protect the public from nation-state threats in cyberspace. In 2017, Microsoft President Brad Smith proposed the adoption of a Digital Geneva Convention that would create a legally binding framework to govern states' behavior in cyberspace.[1] The purpose behind this framework is to establish new rules for governments to aid in the protection of cyberspace during peacetime and prevent nation-state conflicts. Smith's proposal for a Digital Geneva Convention includes ten provisions.[2]

Part 1—Mid-sized Democratic Country Policy Advisor

Section 2. Proposed Amendment. Although the provisions included in Smith's proposal for a Digital Geneva Convention cover a broad range of concepts that are necessary for promoting the stability and security of cyberspace, we suggest the addition of the following provision prior to its consideration for ratification:

The Digital Geneva Convention should commit states to: "*Agree to define what constitutes the use of force within cyberspace through the use of a normative framework*."

Article 2 (4) of the United Nations (UN) Charter prohibits the threat or use of force and calls on all members to respect the sovereignty, territorial integrity, and political independence of other states.[3] Currently, there is no internationally accepted definition of when a hostile act in cyberspace is to be considered as a use of force. In 1999, legal expert Michael Schmitt proposed seven factors dubbed the "Schmitt criteria" to use for determining whether specific malicious cyber-activities meet this qualification: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[4] Schmitt and other authors of the *Tallin Manual on the International Law Applicable to Cyber Warfare* later refined and expanded these criteria to a list of eight assessment factors. These factors, as outlined on the next page, fall under "Rule 11- Definition of Use of Force," which states that a cyber operation constitutes a use

[1] "A Digital Geneva Convention to Protect Cyberspace," *Microsoft Policy Papers* (2017).
[2] Ibid.
[3] United Nations, *Charter of the United Nations*, 1 UNTS XVI (1945).
[4] Schmitt, Michael N., "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Colum. J. Transnat'l L.* (1998): 885.

of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.[5]

1.) Severity: What level of destruction did the operation cause? What was its scope, intensity, and duration?

2.) Immediacy: How soon were the effects of the operation felt? How quickly did its effects subside?

3.) Directness: Was the operation the proximate cause of the effects? Were there other contributing causes leading to those effects?

4.) Invasiveness: Did the operation involve penetrating a cyber network intended to be secure. Was the locus of the operation within the target country?

5.) Measurability of Effects: How can the direct effects of the operation be quantified? How certain is this calculation?

6.) Military Character: Did the military conduct the operation? Were the armed forces the target of the operation?

7.) State Involvement: Is the state directly or indirectly involved in the operation? If not involved, could the state have acted to prevent the operation?

8.) Presumptive Legitimacy: Is this type of operation typically characterized as a use of force? Are the means qualitatively similar to others presumed legitimate under international law?

Section 3. Justification. One expected critique of our proposed amendment is that determining whether a cyber operation should be considered a use of force first requires attribution, which is oftentimes both difficult and time-consuming. We are not suggesting that the UN should be involved in attribution efforts in any way. However, after state governments and private cybersecurity firms successfully determine the malicious actor and layout the full scope of a cyber operation, the UN should use the framework provided in the previous section to adequately assess if it meets the level of a use of force.

Another expected criticism of our proposed amendment is that a few of the assessment factors contained within the framework provided in the previous section are open to interpretation. For example, in reference to the *invasiveness* of an operation, most organizations intend for their systems and networks to be secure, yet they fail to implement the appropriate security measures. Additionally, in reference to the *measurability of effects* resulting from an operation, these tend to be difficult to quantify. As a response to this criticism, we suggest that the UN forms a committee of technical and policy experts from its member states who are responsible for applying the proposed framework.

---

[5] Schmitt, Michael N., ed. *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

Section 4. Conclusion. Overall, our proposed amendment to the Digital Geneva Convention is necessary prior to its ratification, as it would properly distinguish when an act in cyberspace should be considered a use of force, enabling member states to come together and formulate an appropriate response. Additionally, although the proposed amendment does not prohibit the development and maintenance of offensive cyber capabilities, it would likely discourage countries from using them in a manner which would be considered a use of force.

Part 2—Defending Digital Humanity Employee

Section 5. Proposed Amendment. While we support Smith's proposal for a Digital Geneva Convention, we still feel that it fails to provide adequate protection for high-risk users. Therefore, we suggest the addition of the following provision prior to its consideration for ratification:

The Digital Geneva Convention should commit states to: "*Agree to suppress the creation and subsequent use of stalkerware. Governments should require the antivirus industry to issue improved warnings of stalkerware and use their prosecutorial powers to indict executives of companies that produce stalkerware*."

Although provision three of the proposed Digital Geneva Convention encourages the protection of one class of high-risk users, the primary motivation behind this provision is election security. The intent behind our proposed provision is to ensure the digital safety of all high-risk users, not just journalists. Stalkerware refers to tools—software programs, apps, and devices—that allow malicious actors to secretly spy on other individuals via their mobile device.[6] Stalkers need not be skilled hackers to successfully target others—they just need easily accessible consumer spyware and an opportunity to install it on one's device.[7] The recent rise of this industry puts high risk users such as journalists, political activists, and abuse victims at serious risk.[8] Therefore, states must work together to eradicate stalkerware.

One avenue by which states can begin to suppress stalkerware is the antivirus industry. More specifically, governments should require that antivirus software clearly warns users when instances of stalkerware are found on a device. Flagging stalkerware as suspect but "not a virus" as was often done in the past is not enough. Instead, when stalkerware is identified on a device, users should receive an unmistakable privacy alert and be provided with the option to remove this form of malware.[9]

Another avenue by which states can slow the spread of stalkerware is law enforcement. In the United States, existing computer crime laws like the Wiretap Act, the Computer Fraud and Abuse Act, and state-level two-party-consent recording laws apply to a significant portion of stalkerware companies. These pieces of legislation make it illegal to manufacture, sell, or advertise products knowing or having reason to know that its design renders it "primarily useful"

---

[6] "What is Stalkerware?" *Coalition Against Stalkerware*.
[7] "The State of Stalkerware in 2022," *Kaspersky* (2023).
[8] Galperin, Eva, and Morgan Marquis-Boire, "Protecting High-Risk Users," *USENIX Association* (2016).
[9] Greenberg, Andy, "Hacker Eva Galperin Has a Plan to Eradicate Stalkerware," *Wired* (2019).

for the covert interception of electronic, wire, or oral communications.[10] However, many stalkerware companies sidestep these laws by advertising their product as primarily a child-monitoring service, as parents do not need consent from their children to install secret software on their phones.[11] Governments must see through this guise and begin prosecuting stalkerware companies.

Section 6. Justification. One expected criticism of our proposed amendment is that the perpetrators (i.e., individuals who secretly install software on another individual's device without their consent and use it as a tool for spying) should be punished under the law, not the developers of stalkerware. While we agree that the individuals who use this software to stalk and harass others should be subject to criminal charges, it is imperative that those involved in the manufacture, sale, and advertisement of stalkerware also face serious punishment in order to "dry up the source" so to speak. United States federal-level legislation also supports this viewpoint, as highlighted in the previous section.

Another potential critique of our proposed amendment is the difficulty in proving that software is primarily designed for the secret intercept of communications and collection of personal data. Although the producers of stalkerware often market their product as anti-theft or parental control applications, there are certain distinguishing characteristics of stalkerware. Most notably, stalkerware typically operates in stealth mode without users' knowledge and consent. For instance, most stalkerware applications enable perpetrators to hide their app icon from display on the device, enabling for the malicious software to operate in the background. States must recognize this distinct attribute of stalkerware and properly prosecute the executives of companies that produce it.

Section 7. Conclusion. In sum, our proposed amendment to the Digital Geneva Convention is necessary prior to its ratification, as it would better ensure the safety of high-risk users across the globe. The growing popularity of stalkerware continues to put journalists, political activists, and abuse victims in serious danger. Therefore, state governments must rely on their prosecutorial powers along with improved antivirus programs to eradicate the stalkerware industry.

Part 3—UN Secretary General's Assistant

Section 8. Introduction. Prior to any official consideration of the Digital Geneva Convention legislation, we have received two proposed amendments to the initial list of provisions outlined by Microsoft President Brad Smith. The first amendment proposes that we define what constitutes a use of force in cyberspace through a normative framework, specifically the eight assessment factors described in the *Tallin Manual*. The second amendment proposes the eradication of stalkerware through improvements in the antivirus industry and indictments against the executives of companies that produce stalkerware. Given the three fundamental pillars that the United Nations (UN) was originally founded on in 1945—international peace and security, human rights, and development—I support the acceptance of both amendments.[12]

---

[10] Citron, Danielle Keats, "Spying Inc," *Wash & Lee L. Rev* 72 (2015): 1243.
[11] Hautala, Laura, "Stalkerware Sees All, and US Laws Haven't Stopped its Spread," *CNET* (2020).
[12] "The Three Pillars," *United Nations and the Rule of Law* (2019).

Section 9. Proposed Amendment 1 (Mid-Sized Democratic Country). One of the primary functions of the United Nations is to maintain international peace and security, which we achieve through the creation of conditions that allow peace to hold along with conflict prevention. Specifically, Article 2 (4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any state.[13] Therefore, it is pertinent that we define what exactly constitutes a "use of force" within the ever-evolving field of cyberspace. This definition would still provide states the freedom to bolster their offensive cyber capabilities, yet it would likely deter them from using these capabilities in a manner that would meet the "use of force" threshold. Although the normative assessment framework outlined within the *Tallin Manual* is imperfect, a committee of technical and policy experts from member states would possess the prowess to apply this framework appropriately and determine when an action within cyberspace should be considered a use of force.

Section 10. Proposed Amendment 2 (Defending Digital Humanity). Another core function of the United Nations is to promote and protect human rights around the world. The growing popularity of stalkerware globally poses a major threat to high-risk users such as journalists, political activists, and abuse victims.[14] Individuals who end up with this software on their phone experience severe digital privacy intrusions and often become victims of harassment and even physical harm,[15] all clear violations of fundamental human rights. Therefore, the eradication of stalkerware should be an urgent goal. Two clear avenues through which we can work towards achieving this goal are improvements within the antivirus industry, specifically with regard to issuing state-sponsored warnings, and against executives of companies that produce stalkerware.

Section 11. Conclusion. Overall, the proposed amendments for (1) defining what constitutes a use of force in cyberspace and (2) the eradication of stalkerware should both be accepted prior to any official consideration of the Digital Geneva Convention. Although each amendment contains a few limitations, they both support the founding principles of the UN. In conjunction, the two proposed amendments along with the original ten provisions offered by Microsoft President Brad Smith serve to promote responsible state behavior in cyberspace, an urgent priority of the UN.

[13] United Nations, *Charter of the United Nations*, 1 UNTS XVI (1945).
[14] "The State of Stalkerware in 2022," *Kaspersky* (2023).
[15] Greenberg, Andy, "Hacker Eva Galperin Has a Plan to Eradicate Stalkerware," *Wired* (2019).

REFERENCES

"A Digital Geneva Convention to Protect Cyberspace." *Microsoft Policy Papers* (2017). https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

Citron, Danielle Keats. "Spying Inc." *Wash. & Lee L. Rev.* 72 (2015): 1243. https://lawreview.wlulaw.wlu.edu/spying-inc/.

Galperin, Eva, and Morgan Marquis-Boire. "Protecting High Risk Users." *USENIX Association* (2016). https://www.usenix.org/conference/enigma2016/conference-program/presentation/galperin-and-marquis-boire.

Greenberg, Andy. "Hacker Eva Galperin Has a Plan to Eradicate Stalkerware." *Wired* (2019). https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/.

Hautala, Laura. "Stalkerware Sees All, and US Laws Haven't Stopped its Spread." *CNET* (2020). https://www.cnet.com/news/privacy/stalkerware-sees-all-and-us-laws-havent-stopped-its-spread/.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Colum. J. Transnat'l L.* 37 (1998): 885. https://heinonline.org/HOL/LandingPage?handle=hein.journals/cjtl37.

Schmitt, Michael N., ed. *Tallin Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013.

"The State of Stalkerware in 2022." *Kaspersky* (2023). https://securelist.com/the-state-of-stalkerware-in-2022/108985/.

"The Three Pillars." *United Nations and the Rule of Law* (2019). https://www.un.org/ruleoflaw/the-three-pillars/.

United Nations. *Charter of the United Nations*. 1 UNTS XVI (1945). https://www.refworld.org/docid/3ae6b3930.html.

"What is Stalkerware?" *Coalition Against Stalkerware*. https://stopstalkerware.org/.