ifip

Working group 9.10 ICT Uses in Peace and War

Submission to the OEWG

A. Preamble

The work done by both the Open-ended Working Group (OEWG) and the Group of Governmental Experts (GGE) has made significant progress relating to the impact of ICTs on international security. We commend the Chair and the delegations for the work thus far. In principle, we support the Zero Draft, which some minor considerations for adjustment.

However, there is still need for further development in these areas, and reassessment of strategic realities may illustrate gaps that need additional consideration.

This submission will provide points for consideration for the Zero draft, as well as indications where future discussion are required for the topics of International Law; Rules, Norms and Principles for Responsible State Behaviour; Confidence Building Measures; Capacity Building; and other areas that may impact on the work done.

B. International Law

The application of international law to cyberspace should be reaffirmed by the OEWG in the report, in support of GGE's reaffirmation.

To make progress there needs to be a common understanding on the interpretation. For example, how does digital sovereignty differ from sovereignty in physical space? Infrastructure residing in a nation's territory is often mentioned when considering sovereignty; however, important data may reside in another country when cloud computing is employed. Therefore, data sovereignty has different implications to physical infrastructure. These distinctions are important as data can be modified in transit or in storage outside of a national territory, but still affect the national processes. Therefore, we propose that these areas be considered in more detail in future OEWGs with a view of developing international law and its relevance to cyberspace.

The publishing of national perspectives on international law and cyberspace, such as those by Finland[1], France[2], and the Netherlands[3], greatly assists in reaching an understanding of how various nations perceive threats in cyberspace. Even if consensus cannot be reached, mutual awareness of other national positions can aid in avoiding escalation and promoting peace, as well as the development of International Law. We recommend that the OEWG report highlights this transparency for both the purposes of developing international law as well as confidence building measures.

The 2015 GGE Report indicates that states should not use proxies to conduct internationally wrongful acts. This is mentioned in the report; however, we feel that the use of proxies for conducting malicious acts in cyberspace should be more strongly condemned in the OEWG report.

It should be noted that the UN Office of the High Commissioner for Human Rights working group on mercenaries is preparing a report on cyber mercenaries[4]. Once this report is published, it may provide important input into the considerations of international law and cyberspace. There are already blurred lines between military use of cyber capability and the role of private industry. Two examples illustrate this: (1) US Cyber Command reportedly aided in the disruption of a criminal cyber-attack infrastructure[5]; and (2), the SolarWinds incident in which Microsoft played a key part in mitigating the attack [6]. There needs to be further engagements, particularly surrounding the roles of various government agencies (intelligence, law enforcement, and military), as well as civil society, academia and private industry in supporting international security and mitigating malicious use of ICTs in a manner that also protects human rights. We therefore support increasing roles of NGOs in future OEWGs.

C. Rules, Norms and Principles for Responsible State Behaviour

The norms of the 2015 GGE report[7] should be supported and are satisfied with the statements confirming the role of the norms to support international law and guide nations for responsible behaviour in cyberspace.

[1] International law and cyberspace, Finland's national positions, https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859

[2] Ministére des Armées, (2019) International Law Applied to Operations in Cyberspace, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf

[3]The Netherlands: Netherlands Parliament, (2019b) Appendix: International law in cyberspace, 26 September, https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf

[4] See https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx

[5] Greenberg, A. (2020, October 14). A Trickbot Assault Shows US Military Hackers' Growing Reach, Wired, available at: https://www.wired.com/story/cyber-command-hackers-trickbot-botnet-precedent/

[6] Budd, C. (2020, December 16). Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach, Geek Wire, available at: https://www.geekwire.com/2020/microsoft-unleashes-death-star-solarwinds-hackers-extraordinary-response-breach/

[7] Summarised by Esterhuysen, A., Brown, D., and Kumar, S. (2019, 19 December). Unpacking the GGE's framework on responsible state behaviour: Cyber Norms, Global Partners Digital and Association for Progressive Communications, https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/

However, there is a need for expansion of the norms framework, possibly in a hierarchical manner, where various proposed norms from other organisations can be considered as mutually supporting in order to provide depth. For example, the norms of the GGE 2015 report can be used as high-level norms, and norms from the Global Commission on the Stability of Cyberspace (GCSC)[8], Geneva Dialogue[9], and *The Paris Call*[10], can provide norms with more detail or specificity. For example, *The Paris Call* specifically considers election interference, and the GCSC considers non-state actors 'hacking back'. This again illustrates the role for NGOs in future OEWGs.

Whilst there is a concern over influence operations, there are no norms that specifically address disinformation, misinformation, and online influence. The Carnegie Endowment for International Peace has a group investigating influence operations[11]. This is an important aspect as these techniques can be used to directly and indirectly influence sovereign national processes. It is recommended that further discussion be conducted to establish norms relating to influence operations.

D. Confidence-building Measures

Confidence-building measures are an important aspect of international security, and can be used for 'signalling' to mitigate escalation during times of tension. However, deception is a large component of tactics, techniques, and procedures for cyber operations. Therefore, the effectiveness of traditional CBMs may be limited. In particular, cyber capabilities are based on knowledge, therefore it is easier to keep the full extent of offensive cyber capabilities secret than it would be for physical weapons.

NGOs may have a strong part to play in implementing and assessing CBMs. For instance, they can be considered 'neutral', and implement international exercises that can be used both as a CBM as well as capacity building. The 'neutral' posture of NGOs can provide additional support for monitoring of norm implementation and national capacity, as nations may be more willing to provide transparency to an NGO rather than directly to other nations.

E. Capacity-building

We support the capacity building statements in the Zero Draft of the report.

Capacity-building is crucial to effectively maintaining peace online; not only for the traditional technical aspects cybersecurity, but also the legal and diplomatic aspects to cybersecurity. This latter component is particularly lacking. NGOs will have an important role to play in this regard. For example, the CyberPeace Foundation ran a Global CyberPeace Challenge (GCC) 2.0 with a Cyber Policy and Strategy track[12]. Such competitions and similar exercises are important to build capacity and can be used as confidence building measures.

In addition, education is not the only mechanisms for capacity building. Continuous improvement processes incorporating self-assessment and audits to aid in identifying gaps and prioritising areas for improvement can guide the direction of national capacity building. NGOs and international

[8] Global Commission on the Stability of Cyberspace (2019, November). Advancing Cyberstability, https://cyberstability.org/report/

[9] See https://genevadialogue.ch/

[10] *The Paris Call for Trust and Security in Cyberspace* (2018). https://pariscall.international/en/

[11] See https://carnegieendowment.org/specialprojects/counteringinfluenceoperations

[12] See https://www.cyberchallenge.net/cyber-policy-and-strategy-challenge/

collaborations can assist with these efforts. It is recommended that further engagements for capacity building be made, with a view of providing a capability maturity model (CMM) for norms implementation. The CMM can be a basis for guiding self-assessment and continuous improvement.

The inclusion of gender inequality in cybersecurity is welcomed in the report. This can be mitigated to some extent by introducing cybersecurity as a possible career path earlier in education. For example, cybersecurity can be one of the topics covered at STEM awareness and outreach programs, and can be introduced at school level. International collaboration can assist in aiding nations that are still to introduce broad cybersecurity skills development programmes.

As has been noted, the legal and diplomatic aspects of cybersecurity are lacking in skills development, even more so than the more 'traditional' technical skills. Cybersecurity curriculum guidance is provided from the Association for Computing Machinery (ACM)[13] and the *Workforce Framework for Cybersecurity* (NICE Framework)[14]. However, neither of these two explicitly consider international law and diplomacy related to cybersecurity. It is recommended that key topics are identified during further engagements to aid in skills development for cyber diplomacy.

F. General Comments

Whilst the current international law and norms are considered as sufficient, there may still be challenges that arise. International law can gradually adapt to explicitly consider ICTs; however, the current international law is grounded on physical space and distinctions based on the use of force or physical sovereignty. Cyberspace, as indicated above, is not confined by the physical characteristics. In addition, the phrasing often aligns to an escalatory scenario; this may not always be the case. For example, the use of ICTs may be used in an attritional manner, as suggested in the podcasts *Into the Grey Zone*[15]. Individually none of these acts may be considered internationally wrongful, or they could be so subtle as not to immediately raise suspicion. Influence operations may not strictly be internationally wrongful acts; however, prolonged campaigns combined with low-grade cyber-attacks can gradually degrade the decision making of a government, or the confidence in the government. This attritional perspective can therefore be a threat to the processes proposed by the GGE and OEWG, where the confidence building measures are undermined by subtle acts.

G. Summary of Recommendations

Recommendations for the OEWG report:

- The applicability of international law should be explicitly reaffirmed.
- The publication of national perspectives on international law and cyberspace should be further encouraged to support the development of international law as well as a confidence building measure.
- The use of proxies to commit internationally wrongful acts should be more strongly discouraged.

[13] https://cybered.hosting.acm.org/wp/
[14] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
[15] Sky News, *Into the Grey Zone*, Episode 5, available at https://www.youtube.com/watch?v=9huo0PTcQFg

Recommendations for a future OEWG:

- Specific interpretations and development of international law
- The development of an expanded and deeper norms framework
- NGOs have a strong role to play, and greater multi-stakeholder engagement for the next OEWG is proposed

H. Declarations and Authors

This submission is made through the International Federation for Information Processing. The views of the author(s), and does not imply this is the views of the organisation(s) they are affiliated with.

Dr Brett van Niekerk, Chair, Working Group 9.10: ICT Uses in Peace and War, International Federation for Information Processing; Senior lecturer, School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal.

Dr Trishana Ramluckan, Member, Working Group 9.10: ICT Uses in Peace and War, International Federation for Information Processing; Honorary Research Fellow, School of Law, University of KwaZulu-Natal.