Malicious cyber activity against healthcare services and facilities

Joint OEWG Report Proposal from Australia, Czech Republic, Estonia, Japan, Kazakhstan and United States of America. Further supporters of this proposal are invited and welcomed.

Building upon public statements made by many countries to date related to malicious cyber activity during COVID-19 pandemic,[1] the following text is proposed for inclusion in the OEWG report.

Text for the Existing and Potential Threats

States expressed concern about the potential for increased exploitative state-sponsored malicious cyber activity that is inconsistent with international peace and security during global crises, including vis-à-vis critical infrastructure. States noted, with particular concern, reports of attempted and actual damage or impairment by cyber means of the use and operation of critical infrastructure providing services to the public (including healthcare/medical services, facilities and systems, and crisis response organisations) during the COVID-19 global pandemic. States recalled that international law applies to state conduct in cyberspace, as do norms of responsible state behaviour.

Text providing guidance on implementation of norms

(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.

(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 infrastructures, and other relevant resolutions.

> In providing guidance for the implementation of these norms, States should note that highlighting particular sectors as critical infrastructure is not intended to be an exhaustive list and does not impact on the national designation, or not, of any other sector, nor does it implicitly condone malicious activity against a category not specified.
>
> The OEWG developed its report in the context of the COVID-19 pandemic. In these circumstances, the OEWG underscored that all states considered medical services and medical facilities to be critical infrastructure for the purposes of norms (f) and (g).

---

[1] Australia, Chile, Czech Republic, Denmark, Estonia, France, Ireland, Italy, Netherlands, New Zealand, Republic of Korea, Sweden, Switzerland, and the UK included reference to COVID-related malicious cyber activity in responses to the OEWG Pre-Draft Report (see also proposal by ICRC): https://www.un.org/disarmament/open-ended-working-group/. Non exhaustive list of countries that have made standalone statements: Australia (https://www.dfat.gov.au/news/news/unacceptable-malicious-cyber-activity; https://www.zdnet.com/article/australia-and-us-call-out-cyber-attacks-on-hospitals-during-covid-19-pandemic/); Canada (https://www.canada.ca/en/global-affairs/news/2020/04/statement-on-malicious-cyber-threats-to-the-health-sector.html); China http://au.china-embassy.org/eng/fyrth/t1773113.htm); Czech Republic (https://www.nukib.cz/download/publications_en/Warning-NUKIB-2020-04-16.pdf); Estonia (https://vm.ee/en/news/statement-foreign-minister-estonia-urmas-reinsalu-cyber-attacks-against-czech-healthcare); EU: : https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/; Lithuania (https://twitter.com/LT_MFA_Stratcom/status/1251498572828336128); New Zealand: https://www.gcsb.govt.nz/news/new-zealand-condemns-international-cyber-actors-undermining-the-global-response-to-covid-19/; United Kingdom (https://www.gov.uk/government/speeches/foreign-secretarys-statement-on-coronavirus-covid-19-5-may-2020); United States (https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/)