In anticipation of the upcoming sessions of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG II) the CyberPeace Institute (Institute) has set out three key action areas and related recommendations for OEWG II. These recommendations build upon our ‘Statement on the value of multistakeholder engagement in the OEWG process (2021-2025)’ and are forward-looking and action oriented, keeping with the spirit of OEWG II.

Actions and Recommendations aim to address the gaps in capacity and/or knowledge that States have identified themselves, as follows:

**Action Area 1: Healthcare**

Protection of the healthcare sector is an urgent and pressing matter. Access to healthcare is a human right that should be protected as such, and cyber threats can impede upon the enjoyment of this right. In line with the priorities outlined under discussion point one of the First Substantive Session, threats against the healthcare sector need to be studied “...with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats.” During this First Substantive Session the Chair remarked that, “...several States highlighted the vulnerability of the healthcare sector… and noted increased challenges posed by ICT threats to the delivery of essential services.” Ahead of the Second Substantive Session, the Chair asks States to consider how they can “...enhance protection of critical infrastructure, including critical information infrastructure, from existing and potential threats.”

---

Cyber threats to this critical sector have increased dramatically in recent years at a time of additional needs and pressure due to the COVID-19 pandemic. As such, the Institute has the following recommendations for Member States for consideration during the OEWG discussions:

- **Recommendation 1:** Member States should study the continuously evolving threats that the healthcare sector faces, with a particular focus on their impact on individuals. Attacks on this sector have an inherently profound impact upon people. A thorough understanding of the impact upon people is currently missing from threat discussions, especially at the international level. Studying these threats will provide the data and context necessary to effectively respond and increase the overall resilience of the sector.

In an effort to understand the impact of cyber threats, the Institute has been studying attacks against the healthcare sector that can help to inform the work of Member States. For example, since the beginning of the COVID-19 pandemic, the Institute has documented the sharp increase in attacks against the healthcare sector and analyzed the disruption that they cause to individuals. In the first two months of 2022, there have already been at least 28 disruptive cyber incidents against healthcare organizations across 14 countries, signifying a shift away from the US-focus of attacks evidenced in 2021.

For 2022, this is an average of about 3 cyber incidents per week. These incidents, predominantly ransomware attacks, impacted hospitals, national and regional health systems, laboratories and diagnostics centers, and other care providers. As a result, medical and other data have been disclosed making people vulnerable as confidential and personal data has entered into the public domain. As evidenced in the Institute’s incident collection, an attack against a hospital in the United States impacted services, including urgent care X-ray procedures and the organization’s access to email. This illustrates the type of impact upon individuals of a cyberattack, and such attacks occur on a weekly basis.

- **Recommendation 2:** Member States need to increase their own capacity and ability to respond to cyber threats against the healthcare sector. The Institute urges States to analyze past and current initiatives to assess which could be better resourced or scaled to

---


increase the capacity and resilience of the healthcare sector to cyber threats. Lessons can be drawn from past cyberattacks to understand how to better protect the sector. For example, the Conti cyberattack against the Irish Health Service Executive (HSE) has been investigated with results in a publicly available report, so others may also learn from this experience.\(^8\) This Recommendation also aligns with discussion point five on capacity building, and the need to consider specific areas such as incident response and protection of critical infrastructure.\(^9\)

From the non-state actor perspective, the Institute found that its Cyber 4 Healthcare\(^10\) program added value by providing hands-on support to organizations through knowledge sharing and capacity building. Programs such as these provide organizations within the healthcare sector the opportunity to not only gain technical skills, but also to build-up their cyber expertise.

- **Recommendation 3:** Member States should proactively contribute to global capacity building efforts, in line with the agreement under paragraph 59 in OEWG I’s Final Report: “Capacity-building aimed at enabling States to identify and protect national critical infrastructure and to cooperatively safeguard critical information infrastructure was deemed to be of particular importance.”\(^11\)

Several States have launched their own initiatives to not only raise awareness about the threats the healthcare sector faces, but also to share information on best practices that can help to protect this critical sector. For example, in the previous OEWG, the Czech Republic called on Member States to “…proactively contribute to global efforts on critical infrastructure protection, CBMs, and capacity building…”\(^12\) Not only does the Institute

---


urge all States to take on this call to action, but to expand on this call in an effort to protect all designated critical infrastructure sectors.

**Action Area 2: Spyware**

The use of spyware, by both State and non-state actors, without adequate governance and accountability structures and human rights safeguards, is an alarming trend and is undermining the public’s trust in technology. As such, there are several elements that must be addressed in order to comprehensively mitigate the detrimental phenomenon that is spyware-as-a-service. These elements include: focus attention on those who commission, finance, and/or enable such use, and ensure there is accountability. Whether it be probes into government activities or legal action on behalf of vulnerable individuals at the international level, accountability for illicit actions is crucial, especially as the sophistication and use of spyware tools are continually developed.

Over the years a number of organizations including Citizen Lab, Privacy International and Amnesty International have dedicated significant efforts to combat the challenges posed by the spyware market and the impact spyware has on individuals. These organizations have worked on actions such as joint investigations and submission of Amicus Briefs in litigation cases. Through this work, these organizations have raised awareness of the issues, provided ground-breaking forensic methodology reports, and conducted joint advocacy efforts that have promoted legislative actions.

Spyware technology has the capacity to exfiltrate private and confidential information about targets in ways that, if used outside of the framework of permitted interference with human rights (legitimate aim, necessity, proportionality), leads to violations. Moreover, when utilized by governments to target their own or foreign citizens in order to suppress opinion or dissent or illegally gain access to information, it represents a misuse of technology to perpetrate further human rights abuses and undermine democratic values and processes. Cases illustrating this can be found through Forbidden Stories’ “Pegasus Project,” an investigation into the use of Pegasus spyware against journalists, human rights defenders, and politicians, among others. This investigation shows that using unregulated spyware technology has direct risks and impact on individuals, whether they be leaders of nations such as Emmanuel Macron of France,

---


of opposition parties such as Rahul Gandhi of India,\(^{15}\) or journalists such as Marcela Turati of Mexico.\(^{16}\)

Oftentimes, the information obtained using spyware is used to commit further violations of human rights and individual freedoms, such as freedom of the press. The abuse of spyware threatens peace and human security by exposing individuals to persecution.\(^{17}\) As such, the Institute has the following recommendations for State action to study and regulate the production and use of spyware:

- **Recommendation 1: Member States need to bring the topic of commercially available spyware technologies into OEWG II discussions as a present and urgent threat.** At the OEWG, Member States can look beyond individual actors and understand the spyware ecosystem as a whole to present collective solutions that can ensure proper human rights safeguards to the sale, distribution, and deployment of commercial spyware technologies. Spyware is a human security issue, and can therefore fit into the wider, technology-neutral framing of the Human Rights Council’s 2021 resolution on “New and emerging digital technologies and human rights.”\(^{18}\) As not only a present and urgent threat, but a threat to international peace and security, emphasis should be placed on “…the importance of a human rights-based approach to new and emerging digital technologies taking into account States’ obligations under international human rights law, a holistic understanding of technology and holistic governance and regulatory efforts…”\(^{19}\)

For the reasons listed above and specific to OEWG II’s mandate, the use of spyware and its corresponding ecosystem should be considered as an existing threat that warrants further analysis, and can therefore be discussed within the context of discussion point

---


\(^{16}\) “MARCELA TURATI,” Forbidden Stories, accessed March 21, 2022, [https://forbiddenstories.org/journaliste/marcela-turati/](https://forbiddenstories.org/journaliste/marcela-turati/)


\(^{19}\) Ibid.
one, question four, around how States can share information on existing and potential threats.20

- **Recommendation 2: conduct a study on the threat landscape and normative ecosystem of spyware technologies within their territories, and beyond.** This will require a multistakeholder effort, and so the Institute encourages States to turn to civil society, industry, and academic partners in their countries who can support this endeavor. The non-state actor community has extensive knowledge of the threat landscape through in-depth monitoring and provision of statistics on cyber incidents, and can therefore support this work to prevent human rights abuses and to protect rights and freedoms.

Trust in technology is increasingly important in today’s interconnected world. Not only do people need to be able to trust that the technology they rely on every day is secure, but as citizens they also need to trust that their government is using technology in a responsible manner, compliant with their human rights obligations under international law. So far, the use of spyware by governments has undermined this trust, building skepticism among the population, but also leading to wariness between states. In this way, the use of spyware needs to be considered in the context of all present human rights obligations, including those that are extraterritorial in nature.21

- **Recommendation 3: based on the discussions at the OEWG and the study proposed in Recommendation 2, Member States should build capacity in terms of national legislation and policy to regulate the production and use of spyware technologies.** This legislation should keep human rights protections at the core, and focus on ways to protect individuals from becoming targets of spyware technology.

**Action Area 3: Impact of Cyberattacks on Individuals**

The maintenance of international peace and security goes a step further than simply regulating technology; it also needs to consider the protection and enablement of individuals to enjoy their fundamental rights and freedoms and rights to economic and social advancement. As such, studying the impact of potential threats in cyberspace should, first and foremost, mean studying and understanding how their disruptive nature impacts individuals and victims of attacks. It is

---


only by gaining the perspective of individuals and victims through a human centric analysis, that all the areas of the upcoming work of OEWG II will fulfill their ultimate aim. This includes capacity building, implementation of norms of responsible behavior, or confidence building measures. With this in mind, the Institute has the following recommendations to ensure a human centric analysis of cyberattacks:

- **Recommendation 1: Member States, in collaboration with non-state actors, should study the impact of cyberattacks on individuals.** A survey such as UNODC’s Crime Victims Survey\(^22\) or the Crime Survey for England and Wales,\(^23\) can be used as past examples of initiatives aimed at broader understanding of an issue. This endeavor should aim to not only track, but to understand the full scale of this impact. Moreover, this quantification of harm should look beyond economic impact to understand the physical and psychological harm on individuals, and how collectively, this impacts society as a whole. This Recommendation supports discussion point four, confidence-building measures, as it relates to the importance of transparency measures and information sharing; both points included under this section.\(^24\)

- **Recommendation 2: Member States should use findings from the study proposed under Recommendation 1 to inform policy-making, defense measures, capacity building initiatives, and more.** Cyberattacks impact individuals, and so the protection of people needs to be held at the core of these decisions. For policies and laws to be relevant and effective, they need to be based on the reality of the threats and attacks that people are facing everyday.

The CyberPeace Institute believes that these three action areas, and their corresponding recommendations, will aid the ongoing discussions at OEWG II and provide areas for collaboration between State and non-state actors. Ultimately, the peace and security of cyberspace is a collective goal that requires collective action. It is hoped that these Recommendations will be taken into consideration in the Second Substantive Session of OEWG II.

