CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

CyberPeace Institute's Statement

for the fifth session of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG) commenting on the second annual progress report (APR)

Resolution 75/240 mandates the OEWG to submit, for adoption by consensus, annual progress reports to the General Assembly. In accordance with this obligation, the Chair published a zero draft[1] report of the second APR on 13 June 2023, as a starting point for the discussions with delegations and stakeholders, and a revised draft[2] on 12 July 2023 reflecting on expressed preliminary views, with the aim to adopt the APR by consensus at the fifth substantive session that will be held from 24 July to 28 July 2023.

The CyberPeace Institute welcomes the draft APR as a practical outline for future work that proposes concrete steps to advance peace and security in cyberspace and reflects on the recent developments in the field of cybersecurity in the context of international security. Drawing on the Institute's previous submissions to the fourth substantive session that focused on the protection of humanitarian NGOs[3] and increasing transparency around designations of critical infrastructure under confidence building measures (CBMs)[4], as well as the statements delivered at the intersessional meetings[5] and the Chair's informal dialogue with stakeholders[6], the following points are submitted for consideration.

Existing and Potential Threats

Cyberattacks targeting critical infrastructure are increasing in scale and geopolitical significance

It is important to underscore that States have acknowledged that *"a number of States are developing ICT capabilities for military purposes. They also recalled that the use of ICTs in future conflicts between States is becoming more likely, and expressed concern that ICTs have already been used in conflicts in different regions. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States."*[7]

Since the start of the full-scale military invasion of Ukraine on 24 February 2022, the CyberPeace Institute has been aggregating and analyzing data related to cyberattacks and operations against critical infrastructure in Ukraine and the Russian Federation, and affecting non-belligerent countries, as well as data on the perpetrators of such attacks.[8] **The database currently includes cyber incidents perpetrated by more than 100 threat actors in the context of this international armed conflict.**[9]

Due to the lowering of the threshold to conduct cyberattacks and operations, **the threat landscape now consists of nation-State affiliated actors, collectives and hacktivists, and cybercriminal groups**, in addition to nation States as traditional actors. Out of the 2,198 cyberattacks and operations recorded by the CyberPeace Institute to date[10], some 80% are 'self-attributed' attacks. These are cyber incidents in which threat actors publicly disclose the act and attribute themselves as the perpetrator behind the attack.[11] This high level of self-attribution highlights the growing geopolitical importance of cyberattacks against sectors and services deemed essential for States and their populations.

The participation of State-sponsored or affiliated actors and other non-traditional actors in deploying cyberattacks and operations during an armed conflict poses multiple challenges for accountability in cyberspace. Importantly, challenges arise concerning the technical, political, and legal attribution of such cyber incidents, the measures to hold actors accountable for attacks that breach the law, and how these acts set a dangerous precedent for the use of cyber means in future conflicts.

The OEWG should encourage States to increase transparent reporting on cyber incidents, especially those targeting critical infrastructure. Reporting is also pertinent in terms of clarifying how existing and potential threats are experienced differently by diverse sectors, organizations, and communities. Data-driven sharing of information can contribute to raising awareness, increasing cyber resilience across the board, and providing a body of knowledge about the vector, tool, actor(s), and impact of cyber incidents.

States should further engage in focused discussions with stakeholders regarding existing and potential threats that present systemic risks to sectors and services deemed essential. While recognising the need to share objective information on cyber threats in the context of international security in the APR[12], States should further tap into the potential information that can be provided by civil society, industry, and academia. As States expressed concerns that *"a lack of awareness of existing and potential threats and a lack of adequate capacities to detect, defend against or respond to malicious ICT activities may make them more vulnerable"*[13], stakeholders can be trusted partners in supporting national and regional capacities. Private companies, research and civil society organizations, among others, have a proven track record in analysing the threat landscape in a neutral and transparent way, creating repositories of cyber incidents, collecting and investigating such incidents, and mapping their impacts.[14]

Assessing the impacts of cyber incidents necessitates a human-centric approach

The ongoing international armed conflict in Ukraine has been accompanied by an increase in cyberattacks and operations against essential sectors and services across borders and jurisdictions, including beyond the belligerent countries. These have impacted the civilian population and civilian objects, including loss of internet access.[15]

Cyber incidents have an important human component. The APR importantly notes the need for a gender perspective in addressing cyber threats and the specific risks faced by vulnerable groups.[16] The CyberPeace Institute calls on **States to be guided by a human-**

centric approach when assessing the impact of cyberattacks to explain the societal harm of these incidents on people, including groups with specific needs and vulnerabilities. Focused thematic exchanges with stakeholders can foster context-aware approaches to tackling the malicious use of cyber and recognize the various types and levels of harm, and help assess the cumulative effect of cyberattacks on individuals, communities, and society over periods of time.[17]

To advance operationalization of the agreed-upon normative framework through a human-centric approach, **the CyberPeace Institute is developing a methodology to measure the harm caused by cyber incidents**. Through building data-driven understanding of the harm inflicted by cyberattacks, this methodology aims to support policies, strategies and legislation with empirical assessments of their impact. This in turn may increase accountability and help support redress mechanisms for victims of such incidents.

Cyberattacks on humanitarian organizations affect the most vulnerable

Humanitarian organizations are uniquely exposed in cyberspace. On the ground, humanitarian NGOs provide vital support to populations in times of armed conflict, or natural disasters or other emergencies. But their cyber skills, cybersecurity expertise and defenses are generally less robust.[18] The pace of their digital transformation coupled with the limited financial resources available to secure their devices and computer systems put these organizations at a higher risk from cyber incidents.[19]

The humanitarian sector has been adopting digital solutions to reach beneficiaries and scale their services. At the same time, malicious actors target this essential sector to steal funds, surveil or exfiltrate data, including highly sensitive data on vulnerable people, and to disrupt the organizations' ability to operate. Threat actors seek access to data, identify individuals or groups for persecution, conduct hack and leak operations, and carry out ransomware attacks, in order to disrupt humanitarian activities, obtain financial gain, or spread disinformation to undermine the reputation of, trust in and credibility of humanitarian organizations.

Humanitarian organizations are at a stark disadvantage because their cybersecurity budgets are limited and often dependent on donors' contributions. State-sponsored actors, cyber criminal groups and hacktivists threaten NGOs' ability to protect and assist vulnerable populations.[20] Ultimately, **cyberattacks against humanitarian NGOs leave vulnerable people even more vulnerable physically and online**.

States have expressed concern about cyberattacks against humanitarian organizations.[21] The CyberPeace Institute calls on the OEWG to incentivise States to further study threats and impacts faced by the humanitarian sector, as well as facilitate multistakeholder initiatives that gather data to inform the understanding of the cyber threat landscape. Such initiatives and expertise can be instrumental when building knowledge about cyberattacks and their ramifications for society. For example, the CyberPeace Institute is collecting and analysing data about cyberattacks targeting the humanitarian sector as part of its programs and support to NGOs. The Humanitarian Cybersecurity Center[22] is a partnership platform that scales up cybersecurity solutions for humanitarian NGOs. The Center provides expert support and practical assistance to NGOs that is tailored to their needs, and available globally. This work builds upon the CyberPeace Institute's key capabilities and develops programs of activities and associated projects to support communities vulnerable to threats in cyberspace.

The nexus of cyberattacks and the spread of harmful content online

The APR captures concerns of States regarding misinformation and disinformation, in particular where these issues impact international peace and security.[23] **The CyberPeace Institute has observed coordination between cyberattacks and the proliferation of harmful content online**, including disinformation, that creates a convergence presenting unique risks to populations worldwide. This also increases the human impact of cyber threats on vulnerable communities, especially in times of crisis.[24]

Disinformation campaigns can damage trust in public information and institutions, create confusion, and discredit States and organizations alike. Moreover, threat actors can exploit the information ambiguity accompanying armed conflicts, natural disasters, and other emergencies and critical events to further their malicious activities such as phishing attacks, ransomware or hack-and-leak operations, in particular leveraging sensitive and personal data. These campaigns disproportionately impact the most vulnerable, by relying on false information to influence the perceptions of their target audiences, and/or by strategically using the media to disseminate their messages.

This convergence poses risks to populations and amplifies the real-life human impact of threats emanating from cyberspace. It also introduces a new level of complexity that goes beyond addressing individual types of attacks. States should define a roadmap to counter multifaceted threats with an evidence-based understanding of the threat landscape. There should be greater coordination between investigation and research efforts of the private sector, civil society, and academia, and further mainstreaming of cooperation with a variety of stakeholders with relevant expertise.

Rules, Norms and Principles of Responsible State Behaviour

Prioritise practical implementation of cyber norms

Voluntary norms have importance in reducing unpredictability and potential escalation of conflict. However, **the normative framework can contribute to peaceful cyberspace only if it is operationalised by States**, and adopted in their national frameworks and regional strategies. Under the chapter on cyber norms, the APR underlines *"the importance of the protection of Critical Infrastructure (CI). States highlighted that ICT activity that intentionally damages CI or otherwise impairs the use and operation of CI to provide services to the public can have cascading domestic, regional and global effects."*[25] The CyberPeace Institute further welcomes the underlined need for cooperation and assistance as well as the outlined steps "*to ensure the integrity of the supply chain and prevent the use of harmful hidden functions"* and *"promote openness and ensure the integrity, stability and security of the supply chain".*[26] These steps are necessary for States to protect the integrity of supply chains and to maintain a highly secure build and update of infrastructure on which their populations rely.

The CyberPeace Institute has called on States to develop concrete proposals to advance the implementation of cyber norms, especially those with high practical relevance and recognition across countries. We have put forward a series of recommendations in regard to the commitments related to essential sectors and services with the focus on the norm for States to not damage critical infrastructure (norm f) and to protect their own critical infrastructure (norm g) to promote stability in cyberspace.[27] Among other measures, the guidance recommends to States to inform the international community about how they have implemented the norms in their national contexts, or present proposals on the implementation of these norms to serve as guidance to other countries.

We also recommend that States further clarify their views on the application of international law and international humanitarian law in cyberspace to support a comprehensive implementation of the normative framework. This can be, among other measures, advanced when governments and state agencies publicly attribute attacks. Specifying which laws or norms have been violated following a malicious cyber incident that they have attributed to another State would both increase the transparency of attributions and contribute to building capacity of other countries in applying the framework of responsible behaviour.

States can also advance the normative framework by exchanging national views of categories of infrastructure that they assess as priority sectors for broader recognition and increased protection across regions. The OEWG already recognised healthcare infrastructure, medical services and facilities as essential.[28] **Other sectors of critical infrastructure and/or humanitarian organizations can be recognised on a needs-driven and consensus basis to affirm, increase, and incentivise their protection.** Additionally, increased transparency about approaches to designating critical infrastructure can help inform targeted capacity building efforts and build sector-specific understanding by connecting operational realities with the diplomacy and policy levels.[29]

Coupling cyber norms with capacity building and awareness raising

Implementing the normative framework requires targeted capacity building that enhances respective national capabilities. **States should prioritize public-private partnerships, especially in regard to the timely sharing of threat information.** Governments also need to engage in broad multistakeholder consultations that can support their efforts by identifying gaps in current norms implementation. Good practices in this regard include multistakeholder initiatives such as conducting cybersecurity incident exercises, supporting the creation of national or regional points of contact networks, exchanging information in focused discussions, and increasing the capacity of States and stakeholders to contribute to broad accountability in cyberspace.

Civil society organizations play a key role in providing input on the cyber threat landscape, including on issues such as the impact of cyberattacks on human rights, safety and security of people, and implementation challenges of the agreed norms in practice. **The multistakeholder approach is key for building a global culture of cybersecurity and sustainable operationalization of the framework.**

International Law

Clarifications related to the interpretation of international law are still required

States must uphold existing commitments under international law. As agreed in the GGE and OEWG reports, the UN Charter and customary law apply in cyberspace. The CyberPeace Institute noted that the APR reaffirms that *"international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability and promoting an open, secure, stable, accessible and peaceful ICT environment"*[30] and acknowledges the importance of continued discussions on how international law applies to the use of ICTs."

The CyberPeace Institute welcomes the proposal for a compendium of State views[31] and a dedicated intersessional meeting[32] on the applicability of international law in cyberspace, as these formats can encourage States to develop their national views and contribute to developing common understandings on this issue. We further urge the OEWG to encourage more active participation of States in focused discussions with stakeholders, in order to advance clarifications of specific international law-related issues. For example, humanitarian organizations, their staff, and humanitarian data could be considered off-limits for malicious cyber incidents under international law and international human rights law. **The protection**

of humanitarian action under the international legal framework should be ensured and clearly stipulated.

International Humanitarian Law (IHL) reduces suffering online and offline

Cyberspace is not a lawless world, there are rules applicable to cyber warfare that aim to restrain the actions of States and individuals and to protect civilians and critical infrastructure. The International Armed Conflict between Ukraine and the Russian Federation, and its strategic and tactical implications, raise serious concerns and questions about how States and non-State actors respect and abide by the existing legal framework, including domestic law, IHL, and international human rights law. Concerns arise particularly around cyber operations condoned by States that target critical infrastructure and inflict harm on civilians. These attacks undermine the rules-based international order and are inconsistent with States' obligations under international law.

A central tenet of the protection of civilians are the fundamental principles of IHL, which set limits to the ways in which wars are fought. The APR "*recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report*".[33] Under these principles, military force should be proportionate, not excessive, not indiscriminate, and should take all the necessary precautions. Avoiding harm to protected persons and objects is paramount. **As cyber operations are being used as part of armed conflict, States need to further clarify the applicability of IHL, particularly with regards to the limits that existing IHL imposes on cyber operations.** Such additional clarifications would inform the applicability of IHL, protect civilians and civilian infrastructure, and reduce suffering.

States have agreed on the need for further study on how and when these IHL principles apply to the use of cyber capabilities by States.[34] We further encourage States to support multistakeholder partnerships in this regard, as several organizations have built a track record of elaborating how international law applies in cyberspace. They can therefore help States reach common understandings on this issue. The CyberPeace Institute's legal and policy analysis is publicly available on the Cyber Attacks in Times of Conflict Platform #Ukraine[35]. It aims to support States in their work to develop and build upon their national views on how international law applies in the use of ICTs in armed conflict. It also seeks to inform the work of the OEWG. The APR should strongly encourage discussions and cooperation to leverage and expand already existing efforts in this area, in order to support the capacity of States and stakeholders to monitor and call out potential violations of international law in cyberspace.

Confidence-Building Measures

Sharing information is at the heart of building trust between States

CBMs can contribute to incentivizing restraint and de-escalate tensions between and among states, notably by providing transparency and building trust. The OEWG should encourage more active participation in the implementation of the CBMs that have been already agreed upon by GGE in 2013[36] and 2015[37]. The 2015 GGE Report, in particular, includes a CBM on the voluntary provision by States of their national views on categories of infrastructure that they consider critical and national efforts undertaken to protect them.

Voluntarily provided information is the cornerstone of the operationalisation of CBMs. This information can include cyber threats, voluntary sharing of views on international law and its applicability to cyberspace, voluntary sharing of information on national laws, policies, best practices and strategies. It can also include rules and regulations related to cybersecurity, as well as the procedures for information sharing in this area, among other information.

The 2021 GGE report[38] further proposes that States should voluntarily share national views on the classification of critical national infrastructure and critical infrastructure providing essential services regionally or internationally, relevant national policies and legislation, and frameworks for risk assessment and for identifying, classifying and managing ICT incidents affecting critical infrastructure. **The CyberPeace Institute has repeatedly called on the OEWG to encourage States to come forward with clarifications around what they consider essential sectors and services.**

While determining what constitutes critical infrastructure is a national matter, transparency in this regard is important. **Sharing positions on infrastructure considered critical can be**

an opportunity for information sharing and mutual learning toward increased trust in cyberspace. Clarity around what constitutes essential sectors and services would provide incentives and tools for States to advance national frameworks for cyber resilience and exchange best practices and information about targeted capacity building initiatives. Doing so would also promote concrete and actionable cooperation with a broader range of relevant stakeholders in joint efforts to protect sectors and services of critical importance.

Creating a culture of cybersecurity across vital sectors

The involvement of civil society can be particularly valuable in awareness-raising activities about CBMs, their role and implementation on various levels, as well as in contributing to developing a shared taxonomy that can provide a clear definition of the cybersecurity context. The CyberPeace Institute compared the designations of critical infrastructure put forward by some States, finding that their definitions and designations are often too general and prevent building further understandings in regard to operationalisation of normative and legal frameworks. Few States provide a list of sectors considered critical, listing sectors such as nuclear, health, energy or food.[39] Furthermore, as seen in the 2021 OEWG consensus report[40], and acknowledged by the 2021 GGE Report[41], the COVID-19 pandemic led a majority of States to take important further action in protecting healthcare infrastructure.

With infrastructure becoming increasingly digitized, it can be also more vulnerable to cyberattacks. **Determining what constitutes essential infrastructure and how to improve its resilience and protection is important for strengthening accountability in cyberspace.** As the application of IHL can by no means be seen to permit the weaponization of cyberspace, providing transparency around critical infrastructure by no means incentivises the targeting of these sectors. On the contrary, it helps States and stakeholders to join efforts towards greater protection and create a culture of cybersecurity across sectors and services that are vital for our economy and society and that rely heavily on digital means.

Capacity-Building

Towards needs-driven and principled capacity building

Capacity building initiatives should be designed in tandem with the normative and legislative frameworks to achieve their operationalization. In practical terms, capacity building efforts should seek to bridge the gap between States, organizations, and resources and involve all types of stakeholders. These efforts, including information, data, and technologies, which may be part of capacity building, must respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory, transparent, evidence-based and accountable. The CyberPeace Institute urges the OEWG to put particular emphasis on meeting the specific needs of developing countries and to design cyber capacity building programs with norms implementation components.

Capacity building efforts need to support the culture of cybersecurity across the board and existing initiatives should be extended to stakeholders. Many current initiatives are for State participation only. Stakeholders' participation would broaden these initiatives and make them more inclusive, transparent, informed, and impactful. The OEWG can encourage States to engage in broad multistakeholder participation when building cyber resilience, for example, when it comes to vital and under-resourced areas such as the healthcare and humanitarian sectors.

Mainstreaming cyber resilience into the development agenda

The CyberPeace Institute calls on countries to mainstream cyber resilience into the development agenda. To support this objective, we partnered with the Global Forum on Cyber Expertise (GFCE), the World Bank and the World Economic Forum to organize the Global Conference on Cyber Capacity Building under the title "Cyber Resilience for Development"[42]. This event, which will be hosted by the Government of Ghana in Accra on 29-30 November 2023, aims to elevate and mainstream cyber resilience and capacity building in the international development agenda and highlight the key role cyber resilience plays in supporting sustainable development, inclusive economic growth, and social prosperity across regions. The CyberPeace Institute is also a signatory for the joint stakeholder letter[43], which recommends that the APR explicitly states that the OEWG should consider how cybersecurity considerations and good practices can be integrated more broadly into digital development projects.

Regular Institutional Dialogue

The Programme of Action as a way to advance peace and security in cyberspace

The CyberPeace Institute supports the establishment of the Programme of Action (PoA) to advance responsible State behavior in the use of ICTs in the context of international security as a permanent, action-oriented, inclusive, transparent, and results-based mechanism, building on previous outcomes and in line with the cumulative and evolving framework. **The PoA presents a unique opportunity to advance peace and security in cyberspace by assisting the implementation of agreed norms and ensuring practical and needs-driven capacity building.** This initiative should further address a variety of issues related to the operationalization of the agreed-upon framework that would benefit from practical implementation and meaningful multistakeholder participation.

The multistakeholder nature of cyberspace must be reflected in the modalities for stakeholder participation

The inclusion of all relevant stakeholders in a dedicated forum would lend legitimacy and shape any future instrument, such as the PoA. This inclusiveness would create a process that reflects lived realities and addresses real threats that affect the safety, security and well-being of people. Stakeholders can assist States to build their capacity and understanding of how to apply norms on the practical day-to-day level. Civil society organizations in particular are well-positioned to connect different actors and build partnerships across a variety of communities and geographies, in order to help in the practical implementation of cyber norms. They can also assist in national and regional implementation efforts, including reporting on the progress.

While the PoA's modalities when it comes to its scope, method of establishment, format and frequency of meetings, decision-making structures, and stakeholder participation are being debated, **we urge States to create a mechanism that reflects the multistakeholder nature of cyberspace**. Civil society, industry, academia, the technical community, and other experts must be part of any future regular dialogue on cybersecurity in the context of international security. Their engagement and participation will drive more impactful outcomes from the process and contribute to ensuring transparency and credibility of agreed decisions, as well as the sustainability of their implementation.

Collective, coordinated and multistakeholder responses

As States aim to meaningfully progress on the implementation of the agreed-upon framework, the OEWG deliberations must become more granular. **The second APR in its current draft version is a positive step toward incremental but tangible progress.** The OEWG is a State-led process. However, the specificities of cyberspace and the challenges in implementation call for an inclusive process that encourages the participation of a variety of stakeholders.

Addressing cyber threats and the impact and harm they inflict on people will require a collective and coordinated response across diplomatic, policy, civil society and technical communities. The CyberPeace Institute remains committed to supporting and informing the work of the OEWG, in close cooperation with governments and relevant stakeholders, in order to advance accountability, peace and security in cyberspace.

[1] UNODA, "Letter from the OEWG Chair," June 13, 2023, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_13_June_2023_(with_Zero_Draft_Second_APR_enclosed).pdf

[2] UNODA, "Letter from the OEWG Chair," July 12, 2023, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_12_July_2023_(technical_re-issue).pdf

[3] CyberPeace Institute, "Submission on the Protection of Humanitarian NGOs," March 1, 2023, available at: https://cyberpeaceinstitute.org/news/submission-oewg-protection-of-ngos/

[4] CyberPeace Institute, "Submission on increasing transparency around designations of Critical Infrastructure under Confidence Building Measures (CBMs)," March 7, 2023, available at: https://cyberpeaceinstitute.org/news/submission-oewg-designations-critical-infrastructure-cbms/

[5] CyberPeace Institute, "The role of confidence building measures (CBMs) in preventing escalation and strengthening cooperation for international peace in cyberspace," December 5, 2022, available at: https://cyberpeaceinstitute.org/news/the-role-of-confidence-building-measures-cbms/; CyberPeace Institute, "Submission responding to the guiding questions," May 26, 2023, available at: https://cyberpeaceinstitute.org/news/submission-to-the-oewg-may/

[6] CyberPeace Institute, "A multistakeholder response to address cyber threats," July 13, 2023, available at: https://cyberpeaceinstitute.org/news/multistakeholder-response-cyber-threats/

[7] OEWG Second Annual Progress Report, Rev. 1 Draft of 12 July 2023 (hereafter referenced as the "Second Annual Progress Report"), para. 10, part of the "Letter from the OEWG Chair," July 12, 2023.

[8] CyberPeace Institute, "Cyber Attacks in Times of Conflict Platform #Ukraine," available at: https://cyberconflicts.cyberpeaceinstitute.org/

[9] CyberPeace Institute, "From 0 to 100: a story of the escalation of Threat Actors," June 30, 2023, available at: https://cyberpeaceinstitute.org/news/story-of-the-escalation-of-threat-actors/

[10] Last update on June 30, 2023, More information: CyberPeace Institute, "Cyber Attacks in Times of Conflict Platform #Ukraine". Available at: https://cyberconflicts.cyberpeaceinstitute.org/

[11] The Institute does not conduct its own attribution of incidents to identify the actor(s) involved, but documents the attribution efforts by others to link a particular individual, group or state to a specific incident. As there is a reliance on publicly available data, the data on documented cyberattacks in the Cyber Attacks in Times of Conflict #Ukraine Platform gives a classification of certainty based on the reliability of the information source. See the Data and Methodology section of the Platform. More information: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology

[12] Second Annual Progress Report, para. 15.

[13] Second Annual Progress Report, para. 18.

[14] CyberPeace Institute developed two publicly available databases. These repositories of cyber incidents focus on the healthcare sector (Cyber Incident Tracer #HEALTH) and critical infrastructure during conflicts (Cyber Attacks in Times of Conflict #Ukraine). Our Cyber Incident Tracers provide independent, data-driven insights on the cyber threat landscape of the vulnerable communities we serve. They are developed in-house with data sourced through the regular monitoring of open sources by our researchers. The information is made publicly available for use by policymakers, journalists, academic researchers and others and informs our work across the multistakeholder community. More information: https://cyberpeaceinstitute.org/cyber-incident-tracers

[15] CyberPeace Institute, 'Case Study: Viasat', June 2022, available at: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

[16] Second Annual Progress Report, para. 16.

[17] Cyber incidents can have a significant impact on individuals, targeted, or otherwise vulnerable groups in cyberspace. At the same time, they can have lower-level impact but affect people at scale. Harm to populations stemming from cyber incidents can also materialise only after a time delay or may be indirect.

[18] The CyberPeace Institute's research shows that less than 15% of NGOs have cybersecurity experts on their staff, most organizations do not have multi-factor authentication implemented across their IT

environment, and 33% of NGOs do not have dedicated IT resources or security resources available. More information: https://cyberpeaceinstitute.org/humanitarian-cybersecurity-center/

[19] Social Engineering, Ransomware and DDoS attacks are the top 3 types of cyberattacks affecting NGOs who have been targeted in the last three years. More information: https://cyberpeaceinstitute.org/humanitarian-cybersecurity-center/

[20] CyberPeace Institute, "World Humanitarian Day: Safeguarding NGOs against cyberattacks," August 19, 2022, available at: https://cyberpeaceinstitute.org/news/world-humanitarian-day-safeguarding-ngos/

[21] Second Annual Progress Report, para. 10 bis

[22] More information about the Humanitarian Cybersecurity Center: https://cyberpeaceinstitute.org/humanitarian-cybersecurity-center/

[23] Second Annual Progress Report, para. 10 quarter.

[24] CyberPeace Institute, "Quarterly Analysis Report - Q3 July to September 2022," May 3, 2023, available at: https://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q1-2023/

[25] Second Annual Progress Report, para. 22, a.

[26] Second Annual Progress Report, para. 22, b.

[27] CyberPeace Institute, "Protecting critical infrastructure through the implementation of cyber norms," April 26, 2023, available at: https://cyberpeaceinstitute.org/protecting-critical-infrastructure-through-cyber-norms/

[28] For the purposes of norms (f) and (g). The need to affirm the protection of health infrastructure was felt particularly strongly given that the OEWG developed its report in the context of the COVID-19 pandemic.

[29] CyberPeace Institute, "Protecting critical infrastructure through the implementation of cyber norms," April 26, 2023, available at: https://cyberpeaceinstitute.org/protecting-critical-infrastructure-through-cyber-norms/

[30] Second Annual Progress Report, para. 28.

[31] Second Annual Progress Report, para. 32.

[32] Second Annual Progress Report, para. 33.

[33] Second Annual Progress Report, para. 28, b.

[34] Ibid.

[35] CyberPeace Institute, "Law & Policy," available at: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy

[36] United Nations, General Assembly, "Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security," June 24, 2013, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement

[37] United Nations, General Assembly, "Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security," July 22, 2015, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

[38] United Nations, "General Assembly, Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security," July 14, 2021, available at: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[39] Canada uses a risk-based approach for strengthening the resiliency of the country's vital assets and systems. The Government of Canada published the National Strategy for Critical Infrastructure that aims to build a safer, more secure and more resilient ecosystem and advance more coherent and complementary actions among national initiatives on various levels and among the ten critical infrastructure sectors, namely, energy and utilities, finance, food, transportation, government, ICT, health, water, safety and manufacturing. More information: Public Safety Canada, "Canada's Critical Infrastructure," available at: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx;

The US provides a list of what is considered as critical infrastructure. The country recognized 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the country that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety. The list includes the following sectors: chemical, commercial facilities, communication, critical manufacturing, defence industrial base, energy, emergency services, financial services, food and agriculture, government facilities, healthcare and public health, IT, nuclear, transportation systems, and water. More information: US Cybersecurity and Infrastructure Security Agency of the United States (CISA), "Critical Infrastructure Sectors," available at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[40] United Nations, General Assembly," Report of Open-ended working group on developments in the field of information and telecommunications in the context of international security," March 10, 2021, available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[41] United Nations, General Assembly, "Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security," July 14, 2021, available at: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[42] Global Conference on Cyber Capacity Building, available at: https://gc3b.org/

[43] Multiple Groups, "Submission to fifth substantive session by Global Forum on Cyber Expertise," UNODA, July 21, 2023, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Joint_Stakeholder_Letter_on_Capacity_Building_in_the_OEWG's_Second_APR.pdf