Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025

4th Substantive Session

Collection of Statements by the Paris Peace Forum

- **Informal Dialogue Between the Chair and Interested Stakeholders – 1st March 2023**

The Chair invited **focused discussion existing and potential threats in the field of ICT security.**

Thank you, Mr. Chairman, distinguished Delegates and dear participants,

My name is Jerome Barbier and I am speaking on behalf of the Paris Peace Forum, which welcomes the secretariat of the Paris Call for Trust and Security in Cyberspace. The Paris Call is one of the world's main multistakeholder platform to advance norms and principles to common norms and principles to defend accountability and human security in cyberspace, thanks to its community of over 1200 supporters from across the ecosystem.

Mr. Chairman, allow me to first reiterate our appreciation for your sustained efforts to ensure the participation of all interested stakeholders in the work of this Open-Ended Working Group, including through today's informal dialogue. In line with the fundamental parameters of cyberspace, which is privately owned and operated for a significant part, stakeholders are in a position to provide critical expertise that can usefully inform multilateral discussions, as well as contribute to the full implementation of the resulting norms, principles and guidelines adopted by States. This is particularly true when it comes to identifying and analyzing emerging dynamics in the ICT environment that may constitute a threat to international peace and security. We thus regret the persisting politization of stakeholder participation in the OEWG process, which only deprives States from first-hand expertise and experience of ICT security.

Starting in 2022 and onwards, the Paris Call community has in this regard leveraged its 1200-wide, public-private community to focus on risks resulting from uncontrolled proliferation of malicious

software and practices intended to cause harm - a growing, multifaceted trend insufficiently addressed by current international and national frameworks. The incompressible presence of exploitable vulnerabilities within the ICT environment makes it a particularly fertile ground for such proliferation, fueled by a diverse set of malicious actors, including State-backed groups, criminal organizations and "access-as-a-service" mercenaries. Such activities, whether driven by political or purely lucrative intents, not only endanger the global stability of cyberspace but also have increasingly harmful consequences for civilian populations over the world. Emerging technologies such as quantum capacities or large-scale mature applications for artificial intelligence will most certainly further accelerate this well-established adverse dynamic. As mentioned by other stakeholders today and while dealing with the genuine risks posed by emerging threats, we also encourage States to consider that break-through technologies will first and foremost strengthen existing malicious cyber activities.

The dual nature of most technologies involved, as well as the difficulty to determine any actor's intentions in cyberspace with a reasonable degree of confidence, call for innovative and tailored approaches to tackle this issue, for which current frameworks and inspiration from more traditional arms control fields are at best insufficient, at worst ineffective. Many reports emanating from civil society, academic experts but also from the private sector over the past years unfortunately support this observation. The diversity of fora, markets, and jurisdictions through which malicious software and practices proliferate, as well as the essentially private ownership of the technologies being diverted for such uses, requires a global, joint and multilayered effort by all relevant actors around the Globe - including policymakers, regulatory authorities, law enforcement agencies, industry, academia and civil society organizations.

The Paris Peace Forum welcomes in this regard successful work undertaken in the framework of the United Nations such as the *UN Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination*, as well as other initiatives lead by a number of States such as the *Export Controls and Human Rights Initiative*. In the same way, we welcome efforts at the regional and global level to build effective Coordinated Vulnerability Disclosure frameworks that can foster cooperation between jurisdictions and between the public and private sector for this purpose, while providing adequate protection for security researchers. A remaining challenge is to efficiently articulate existing initiatives in order to avoid silos and to grasp this trend in a comprehensive manner, with meaningful inclusivity as a condition for success.

We therefore call on the community of States as a whole to embrace this issue by giving substance to Article 11(i) of the 2015 GGE report according to which "*States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions*". The wider stakeholder community should also be able to fully participate in this endeavor, to ensure both the relevance and efficiency of any agreed solution.

In the coming years, The Paris Call's community will strive to broadly mobilize within the ecosystem, primarily within its multistakeholder community, to identify effective formats to counter such proliferation and thus to reduce benefits while maximizing costs for malicious actors who seek to undermine our collective security in cyberspace.

- **Informal, dedicated stakeholder segment – 9th March 2023**

The Chair invited **focused discussion on best practices and lessons learnt on the topic of public-private partnerships** for capacity-building in the area of security in the use of ICTs:

1. *Are there good examples of public-private partnerships on capacity-building in the area of security of and in the use of ICTs?*
2. *Are there lessons that can be gleaned from those examples?*

Thank you, Mr. Chairman, distinguished delegates,

The relevance of public-private partnerships for cyber capacity building has been extensively justified in theory, and successfully experienced around the Globe. The Paris Peace Forum would however like to address a common limit in approaching public-private partnerships in this area.

Public-private partnerships for cyber capacity building are indeed often approached at the stage of policy implementation, as the strengthening of States and stakeholders legal and technical capacities. They are yet as relevant at the stage of policymaking, by leveraging the expertise and experience of the larger stakeholder community, including the private sector, organizations from the civil society and in particular academic institutions, as well as technical experts to increase States policy capacities – especially when it comes to tackling emerging threats. The Paris Peace Forum will thus focus on recalling successful examples of large, multistakeholder cooperations in the making of cyber policies.

Cooperation undertaken in the framework of the Global Forum for Cyber Expertise, whose role and achievements have been acknowledged by many delegations this morning, is an obvious example. While providing comprehensive resources and support to strengthen legal and technical capacities across the Globe, GFCE working group A specifically focuses on increasing policy and strategy making capacities. This for instance led to the development of the online "", a detailed framework and set of resources to help national actors designing their national cyber policy.

On the more precise issue of ransomware threats, the Ransomware task force established in 2021 and hosted by the Institute for Science and Technology is another example of successful public private partnership in cyber policy capacity building. The Task Force has aimed to unite and build trust between key stakeholders across industry, government, and civil society, to innovate new solutions, break down silos, and find effective new methods of countering the ransomware threat. This led to making of a large range of actionable policy recommendations increasing public authorities' ability to build strategies and policies to address the ransomware phenomenon.

In this endeavor, the role of informal diplomacy shall finally be emphasized. Non-institutional fora and non-governmental organizations such as the World Economic Forum, the Raisina Dialogue, or the Paris Peace Forum enable States to benefit from informal engagement with stakeholders, even on sensitive policy issues. In this regard, they are critical resources to increase States cyber policy capacities, and are complementary to formal negotiations and processes undertaken in the framework of the United Nations.

In the same way, existing multistakeholder frameworks such as the Cybersecurity Tech Accords or the Paris Call for Trust and Security in Cyberspace can be leveraged to increase political awareness on cyber policy, and confirm priority directions to build robust and resilient national cyber strategies.

I will conclude by thanking you, Mr. Chair for your commitment to engage meaningfully with the stakeholder community, as part but also beyond the substantive session of the OEWG.