Wednesday, 20 September 2023

**His Excellency Ambassador Burhan Gafoor**

Chair of the Open-Ended Working Group

on security of and in the use of information

and communications technologies 2021-2025

C/O The Secretariat of the OEWG

Office of Disarmament Affairs

prizeman@un.org

New York

Dear Chair, distinguished Delegates,

We, the undersigned organizations and experts, commend States for the consensus reached on the second Annual Progress Report of the United Nations (UN) Open-Ended Working Group (OEWG) on the security of, and in the use of the information and communications technology (ICT) environment. However, we express our deep concern about the exclusion of references to cyber mercenaries, irresponsible use of access- and hack-as-a-service solutions.

Cyber mercenaries, companies that offer offensive cyber capabilities to enterprises and governments for a fee, often promote their offerings under the pretext of countering terrorism or as a means to pursue other legitimate national security goals. Yet, their products and services often exceed these purposes, threatening global cyber stability.

Cyber mercenaries contribute to the rapid and uncontrolled proliferation of offensive capacities by stockpiling and exploiting vulnerabilities to develop their products and services. They search for ways to access networks without authorization, maintain a surreptitious presence on a device or system, and exfiltrate or destroy sensitive data potentially putting millions of users at risk – including government users.

Even more worryingly, their methods can weaponize the internet infrastructure, making the entire digital space a legitimate target for their opponents. This may lead to further fragmentation of cyberspace worldwide, as it may prompt some States to consider justifying extreme, unlawful measures such as banning whole services, imposing blanket internet shutdowns, or deploying even more intrusive cyber surveillance tactics as legitimate countermeasures.

The unchecked growth of the cyber mercenaries' marketplace poses a direct and serious threat to the stability of the ICT environment in both the short and long term - reason why it must be addressed at both national and international levels. The tools and techniques they sell clearly violate the framework of responsible State behavior in cyberspace, endorsed by consensus through multiple General Assembly resolutions – including norms 13 (a), I, (i) and (j) of the 2015 and 2021 UN Group of Governmental Experts (GGE) report, endorsed by UN General Assembly resolution 70/237 and recalled in the OEWG second Annual Progress Report.

We call on States to prioritize this pressing issue in next year's OEWG convenings. Instead of watering down references to one of the main threats to cyber stability, we urge States to confront this major challenge directly as a critical example of irresponsible use of the cyberspace. In doing so, States can leverage existing initiatives undertaken in this regard, including those led by the multistakeholder community.

***Signatories:***

- **Paris Peace Forum** – Acting as secretariat of the Paris Call for Trust and Security in Cyberspace, the Paris Peace Forum is coordinating a multistakeholder working group focusing on identifying the modus operandi of cyber mercenaries, clarifying economic dynamics at stake and better measuring effects from an international security perspective. Preliminary findings will be unveiled at the 6th edition of the Paris Peace Forum in November 2023, paving the way towards the formulation of code of conduct to articulate the responsibility of all relevant actors from the ICT environment.

- **APCO Worldwide –** APCO Worldwide is an advisory and advocacy communications consultancy helping leading public and private sector organizations be catalysts for progress by navigating the challenges of today. Four years after its launch, APCO was asked to act as the Tech Accord's Secretariat. As such, it provides strategic guidance and support to evolve the group from a platform that drew an audience of policy makers and industry peers into an open space for dialogue, directly engaging consumer audiences.

- **Cybersecurity Tech Accord –** Launched in 2018, the Cybersecurity Tech Accord is a coalition of more than 150 global technology companies committed to foundational cybersecurity principles for responsible industry behavior. In the years since, the coalition has served as the voice of the technology industry in discussions around peace and security online as the world has continued to sleepwalk into seemingly ever-escalating cyber conflict. On March 2023, the Tech Accord released a new set of principles to guide the technology industry to help curb the dangerous and rapidly growing market of "cyber mercenaries".

- **CyberPeace Institute – The** CyberPeace Institute is a Geneva based organization protecting the most vulnerable in cyberspace. Independent and neutral, the Institute investigates and analyzes the human impact of systemic cyber threats, delivers free cybersecurity assistance, tracks the enforcement of international laws and norms and forecasts threats to cyber-peace. The Institute has long experience of advocacy and research on the issue of cyber-mercenaries.

- **DXC Technology –** DXC Technology Company ("DXC") is a global technology service provider located in over 70 countries Services provided to customers include cybersecurity, but DXC also maintains a robust cyber program designed to protect its own internal systems, applications and proprietary data worldwide. DXC is a strong advocate for the private sector to engage with international stakeholders as governments and their constituents work to establish international norms, laws and regulations applicable to cyber events. Accordingly, it has actively engaged as informal participants in the OEWG since 2019 and has been an active contributor to the Paris Call as well as other industry interest groups and consortiums.

- **Hague Centre for Strategic Studies** – The Hague Centre for Strategic Studies (HCSS) is a knowledge institute that conducts independent research. Its goal is to offer fact-based analysis of the challenges that our societies face in order to inform public discourse, public and private strategic decision making and contribute to international and national security in accordance with liberal democratic values. They conduct research at the intersection of scientific research and strategic policy for governments, international organizations, and NGOs. The HCSS calls for cyber-transparency as a precondition for preventing misjudgments of cyber threats and policy interventions. In 2022, The HCSS released the Cyber Arms Watch, offering a transparency index on the offensive cyber capabilities of 60 states.

- **ICT4Peace Foundation** – A pioneering organization dedicated to promoting peace and security in the digital age, the foundation has been addressing the challenges posed by cyber threats and conflicts while highlighting the potential of information and communication technologies as tools for peacebuilding and conflict resolution since its beginnings at WSIS 2003. By bridging the gap between technology experts, policymakers, and peace advocates, ICT4Peace aims to shape a safer and more harmonious digital future for all.

- **International Chamber of Commerce –** As the institutional representative of over 45 million businesses, reaching more than 170 countries, the International Chamber of Commerce (ICC) operates with a mission to make business work for everyone, every day, everywhere. The business community is committed to ensuring the security of cyberspace. ICC calls on the international community to build on that commitment by more effectively addressing the ever-growing frequency and intensity of cyberattacks through international cooperation, including by addressing the proliferation of offensive cyber capabilities.

- **Microsoft –** Microsoft is a technology company with over forty years of experience developing products and services across the ICT landscape for customers around the world. Today, this includes operations focused on personal computing, cloud services, gaming, the Internet of Things (IoT) and others which are increasingly threatened by malicious cyber activities. As one of the world's leading providers of ICT infrastructure, Microsoft is on the front lines of the global effort to defend against cyberattacks directed at organizations of all kinds. It has been instrumental in raising global awareness on the need to curb the cyber-mercenary market, including through its active participation in the Paris Call and the Cybersecurity Tech Accord.

- **U.S. Council for International Business –** The United States Council for International Business (USCIB) is an independent business advocacy group that was founded in 1945 to advance global interests of American business, in particular within intergovernmental fora. USCIB's advocacy spans a broad range of policy issues, leveraging the expertise of our business members and a network of global business organizations: the International Chamber of Commerce (ICC), Business at OECD, and the International Organization of Employers (IOE).

***Signatories on an individual capacity***:

- **Allison Pytlak –** Cyber Program Lead, The Stimson Center