NOVEMBER 2023

TAMING THE CYBER MERCENARY MARKET

A Multistakeholder Blueprint Towards Increased Transparency and Cyber Stability

PARIS CALL WORKING GROUP ON UNPACKING THE CYBER MERCENARIES' PHENOMENON

PARIS CALL
For trust and security in cyberspace

PARIS PEACE FORUM
de PARIS sur la PAIX

In an era where States are increasingly leveraging cyber capabilities for strategic and national security objectives, the recourse to external suppliers has become commonplace. As a result, a rapidly growing market for offensive cyber tools and services has developed to meet this demand, which, if left unregulated, may present a direct threat to global cyber stability and peaceful use of information and communication technologies.

These "cyber mercenary"[1] companies offer tools and services that are potentially exploited not just by governments, but also by certain non-State actors. Targets include journalists, human rights defenders, political dissidents, government officials and industry representatives around the world for surveillance purposes, as well as infrastructures to conduct destabilizing operations in and through cyberspace. By weaponizing such technologies, these firms also expose countless others to security threats, eroding trust in the digital realm. A growing number of countries recognize the threat posed by cyber mercenaries, including the misuse of commercial spyware, and the need for strict domestic and international controls on the proliferation and use of such technology. The wider stakeholder community has also addressed this phenomenon in recent years through joint initiatives and key studies, contributing significantly to clarifying the dynamics at play and boosting global momentum.

Against this backdrop, the multistakeholder community of the Paris Call for Trust and Security in Cyberspace will establish a Working Group in 2023 to delve deeper into the Cyber-Mercenaries phenomenon and develop action-oriented policy proposals to address this escalating challenge. As foundational pillars, we as participating supporters of the Paris Call:

- Reaffirm our support to an open, free and secure cyberspace,[2] and the responsibilities of all pertinent actors to ensure global cyberstability;
- Reaffirm the Paris Call for Trust and Security in Cyberspace founding declaration and recall Principles 1 on Protecting individual and infrastructure, Principle 5 on the Non-Proliferation of malicious software and practices intended to cause harm, and Principle 8 on Preventing non-state actors from hacking back as particularly relevant in this context;
- Reaffirm that international law, including the United Nations Charter in its entirety, international humanitarian law, and customary international law are applicable to the use of information and communications technologies.[3] We specifically highlight the importance of international human rights law and international humanitarian law in this context;
- Recognize the responsible use of commercially available active cyber tools and techniques both for cybersecurity purpose, such as testing the robustness of a software or an information system, and for the fight against organized crime and terrorism;
- Express concern about the risks and abuses posed by an unregulated cyber mercenaries' market as antithetical to the principles of the Paris Call, as the proliferation and irresponsible use of cyber mercenaries' tools and services may result in significant, indiscriminate or systemic harm to individuals and/or critical infrastructure;[4]

---

[1] For the purpose of this document, Cyber Mercenaries is defined as formal and informal entities that offer cyber capabilities and services primarily for intrusive purposes to governments and non-State actors targeting a third party. The offered capabilities and services, such as commercial spyware, aims to provide various forms of access on targeted third-party's ICT systems without the consent or knowledge of this system's owner, with the view to surveil, capture or manipulate data. This definition therefore does not include cyber capabilities and services which, although they present an intrusive element, fall within the broader defensive context of enhancing buyers' level of cybersecurity.

[2] The Paris Call of the 12 November 2018 — Paris Call

[3] The Paris Call of the 12 November 2018 — Paris Call

[4] The Paris Call of the 12 November 2018 — Paris Call

- Stress that all actors can help address this issue through the responsible reporting of vulnerabilities, as called for in norm '(13-j)' of the 2015 UN Group of Governmental Experts (GGE) report[5] and in the UN Open-ended Working Group on cybersecurity (OEWG) 2021 second Annual Progress Report[6], as endorsed by the UN General Assembly.
- Welcome existing efforts by states to take steps to curb the cyber mercenary market, including the United States' Executive Order on the Prohibition of the Use of Commercial Spyware That Poses Risks to National Security,[7] and the commitments outlined in the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware released during the 2023 Summit for Democracy, as well as the initiative taken by France and the United Kingdom to initiate an international process on the threat posed by the proliferation and irresponsible use of advanced commercial cyber tools and services[8];
- Recognize the updates made to the control list of the Wassenaar Arrangement on Export Control for Conventional Arms and Dual-Use Goods and Technologies to include intrusion software in 2013[9], as well as other relevant regional export control frameworks that covers similar capabilities;
- Recognize the work of the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee);[10]
- Highlight the 2022 report of the UN Working Group on the use of mercenaries;[11]
- Recognize the civil society and independent experts call for states to implement an immediate moratorium on the sale, transfer and use of surveillance technology;[12]
- Underline the civil society call to ensure all companies, including VC firms, domiciled in their countries are required to undertake human rights due diligence in respect of their global operations and investments. The same should apply for companies that seek to do business within their domestic jurisdictions. This includes comprehensive transparency requirements for investors, including public disclosures from VCs about their investments.[13]
- Welcome efforts by states and non-state actors to provide support to victims of malicious use of information and communication technologies[14], including victims of the hack- and access-as-a-services industry.
- Recall the responsibility of private sector actors in improving trust, security and stability in cyberspace, including through responsible development of their products and services, and

---

[5] United Nations General Assembly, Doc A/70/174, July 2015

[6] Microsoft Word - Final report A-AC.290-2021-CRP.2.docx (un-arm.org)

[7] Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security

[8] Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware | The White House

[9] Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, December 2022

[10] REPORT of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware | A9-0189/2023 | European Parliament (europa.eu)

[11] UN OHCHR | Report of the 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 | The human rights impacts of mercenaries, mercenary-related actors and private m

[12] Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology - Amnesty International

[13] Joint Statement: States & investors have a responsibility to curtail the abuse of spyware

[14] The Paris Call of the 12 November 2018 — Paris Call

encourage initiatives aimed at strengthening the security of digital processes, products and services;[15]

- Recognize the multifaceted nature of the cyber mercenaries' phenomenon and the need for sustained multi-stakeholder collaboration to curb this threat – as highlighted in the above reports and initiatives and in line with the Paris Call's broader purpose.

With grave concerns about the growth of the "cyber mercenary" market and following this first year's reflection, Working Group's participants recommend implementing the following priority measures aimed at addressing some of the greatest risks posed by the cyber mercenaries' phenomenon:

- *Develop clear acceptable use guidelines:* Governments' use of cyber mercenaries' tools and services, including commercial spyware, should follow clear guidelines on responsible use. Recourse to cyber mercenary tools and services must be carried out in accordance with States' domestic law, international obligations and commitments and incorporate principles such as legality, necessity, proportionality and distinction.
- *Safeguard ICT exports from malicious use:* Governments should cooperate to prevent the export of software, technology, and equipment to end-users who are likely to use them for malicious cyber activity, including unauthorized intrusion into information systems, in accordance with the respective legal, regulatory, and policy approaches and appropriate existing export control regimes.
- *Prevent purchases by non-State actors:* Companies and governments should prohibit the sale or transfer of cyber mercenaries' software, technology, and equipment to non-governmental actors, in accordance with the respective legal, regulatory, and policy approaches and appropriate existing export control regimes.
- *Require oversight:* Companies and governments should adopt appropriate internal oversight mechanisms that help ensure compliance with domestic laws, procedures and policies along with applicable international human rights obligations.
- *Adopt transparent procurement practices:* Governments should be transparent in their procurement practices, requiring vendor consistency with the UN Guiding Principles on Business and Human Rights;[16] define the safeguards in place to prevent abuse or discriminatory uses; and enhance their reporting practices with regard to such transactions.
- *Mandate vendor verification:* Governments should establish and publicize monitoring and verification procedures for ensuring that cyber mercenaries – particularly those who are its nationals, residents, or contractors – are in accordance with all applicable domestic and international laws.
- *Blacklist violators*: Governments should consider blacklisting cyber mercenaries who violate relevant international norms and human rights, including by restricting access to particular markets.[17]
- *Develop guardrails for former government employees*: Governments should identify proper restrictions for individuals previously employed in sectors such as the military, intelligence, law enforcement, or other national security or cybersecurity roles. These restrictions, aligned with domestic laws and policies, should address the transition of former government employees to the private sector, with special attention paid to private sector roles that are involved with commercial

---

[15] The Paris Call of the 12 November 2018 — Paris Call

[16] Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework | OHCHR

[17] Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, 2021

spyware sales. To help ensure security and reduce risks, measures could include mandatory reporting for post-government employment, specific employment restrictions and relevant training programs.

- *Respect the Cybersecurity Tech Accord industry principles:*[18] Industry partners should respect the co-developed principles that task companies to 1) take steps to counter cyber mercenaries' use of products and services to harm people; 2) identify ways to actively counter the cyber mercenary market; 3) invest in cybersecurity awareness of customers, users and the general public; 4) protect customers and users by maintaining the integrity and security of products and services; and 5) develop processes for handling valid legal requests for information.
- *Vulnerability discovery and handling:* Industry partners should strive to strengthen their collaboration with relevant stakeholders, including good faith researchers from academia and civil society, to improve the discovery and handling of vulnerabilities embedded in their products and services on an ethical and responsible basis. In particular, Industry partners may establish, improve and harmonize coordinated vulnerability disclosure processes as well as to operate bug bounty programs.
- *Publish evidence-based findings to contextualize threats:* Industry partners and civil society organizations should continue generating evidence-based insights for better transparency and accountability of cyber mercenaries and their clients. Understanding the risks and threats posed by these groups will help create effective guardrails for responsible use set the foundation to limit the market.
- *Expand collective knowledge of the market:* Civil society and academic actors should work together to increase our common knowledge about the cyber mercenary markets, including economic dynamics and market trends at stake, to identify most efficient policy levers to further counter the proliferation of cyber offensive tools and services.

Without strict boundaries, the unchecked growth of the cyber mercenary market and irresponsible use of these capabilities, including commercial spyware, will lead to significant harm and systemic instability in cyberspace. To address this, we advocate for increased partnerships across government, industry, and civil society sectors, enhancing awareness and building capacity to address the issue.

In order to monitor the progress made in implementing the above principles and commitments, we invite the Paris Call stakeholders to reconvene and report on their actions at the 2024 edition of the Paris Peace Forum.

We collectively call on all interested stakeholders to build on these recommendations, to raise awareness about them, and to take action to prevent irresponsible use of advanced commercially-available active cyber spyware tools and services.

[18] Cybersecurity Tech Accord's industry principles, March 2023

Composition of the Working Group

This Working Group gathered experts representing formal supporters of the Paris Call for Trust and Security in Cyberspace as well as other authoritative institutions in the field of cyber security and stability. This document summarizes the main priority recommendations debated during the first year of work and agreed by consensus. Participation in the Working Group shall not be regarded as formal endorsement.

CyberPeace Institute*
Switerland
Charlotte Lindsey

Chatham House
United Kingdom
James Shires

Cybersecurity Tech Accord
Edoardo Ravaioli

Durban Institute of Technology
South Africa
Brett van Niekerk

France
Mahé Dersoir

HCSS ***
Netherlands
Michael Rademaker

ICT4peace
Switzerland
Anne-Marie Buzatu

Microsoft
United States
Monica Ruiz

Stimson Center
United States
Allison Pytlak
James Siebens

University of KwaZulu-Natal
South Africa
Trishana Ramluckan

Observers

CEIP **
United States
Tim Maurer

United Kingdom
Benjamin Walden
Kirsten Holden
Helen Mcleod

UN ODA
United Nations
Beyza Unal

**Co-Chair of the Working Group
Carnegie Endowment for International Peace | * Hague Centre for Strategic Studies

ABOUT THE PARIS CALL

The Paris Call for Trust and Security in Cyberspace, launched at the 2018 Paris Peace Forum, has become the reference multi-actor framework to advance common norms and principles for peace and security in cyberspace. Five years after its launch, it is now supported by more than 1200 actors, including 80 states, 700+ companies, and 380+ civil society organizations, rallied around nine common principles to defend a free, open and secure cyberspace through enhanced multistakeholder collaboration.

ABOUT THE PARIS PEACE FORUM

In a world requiring more collective action, the Paris Peace Forum is a platform open to all seeking to develop coordination, rules, and capacities for concrete solutions to global problems where none exist. Year-round support activities and an annual event in November help better organize our planet by convening the world, boosting projects, and incubating initiatives.

PARIS CALL
For trust and security in cyberspace

PARIS PEACE FORUM de PARIS sur la PAIX