****

Tackling the Proliferation and Irresponsible Use

of Cyber Intrusion Capabilities

Drawing a multi-stakeholder agenda in the wake of the Pall Mall Process launch

**OEWG Seventh Substantive Session**

On February 6th, France and the United Kingdom started the [Pall Mall Process](https://assets.publishing.service.gov.uk/media/65c25bb23f6aea0013c1551a/The_Pall_Mall_Process_tackling_the_proliferation_and_irresponsible_use_of_commercial_cyber_intrusion_capabilities.pdf), an international effort aimed at exploring policy options and new practices to tackle the threat posed by commercial cyber proliferation and irresponsible use of cyber intrusion tools and services. This joint effort, supported by 25 States alongside industry partners and civil society organizations, builds on the discussions held during the 2023 edition of the Paris Peace Forum and follows the [multistakeholder work](https://parispeaceforum.org/publications/paris-call-taming-the-cyber-mercenary-market/) conducted under the Paris Call for Trust and Security in Cyberspace from the past year. It further contributes to the growing interest on this issue in every part of the world since 2022.

An effective response to the proliferation and irresponsible use of commercially available cyber intrusion capabilities faces the remaining challenge of universalizing the effort and striking a fair balance with the right of States to ensure their own security. It may also require coordinating the existing efforts among the wider stakeholder community. In addition, consideration should be given to how these efforts can be reflected in the work of multilateral processes, beginning with the 2021-2025 Open-ended Working Group.

This private workshop will bring together the Paris Call supporters who are involved in the Cyber Mercenary working groups with the entities that attended the inaugural conference of the Pall Mall process. They will work together to identify the priority areas, gaps and challenges that need to be tackled in 2024 for an effective action against the spread and misuse of cyber offensive capabilities that are commercially available - before the 2025 Pall Mall meeting hosted by France. Participants will also be invited to discuss how to connect this initiative with the existing and ongoing work on ICT security at the United Nations. Particular attention will be paid to how best to coordinate the actions of non-state actors to make a significant contribution, including through platforms such as the Paris Call.

**List of invitees:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **States & IO** | **Industry** | **Civil Society** |
| **Present for Pall Mall (signatory in bold)** | * Vietnam * Brazil * **Malaysia** * **African Union** | * **BAE systems** |  |
| **Paris Call Supporter** | * Cyprus * Morocco * European Union * Interpol | * CISCO * DXC Technology * International Chamber of Commerce * Thales | * Access Now * Global Forum on Cyber Expertise * Chatham House * School of International Information Security, Institute of Contemporary International Studies, National Univeristy of Singapore * Red en Defensa de los Derechos Digitales * Carnegie Endowment for International Peace |
| **PM+PC** | * United Kingdom * France * United States * Greece * Switzerland * Singapore * Japan | * Microsoft * Google * Meta * HackerOne * Margin Research * Yes We Hack * Sekoia.io | * GEODE * Stimson Center * ICT4Peace * CyberPeace Institute * Atlantic Council * RUSI |

**+ UNODA and UNIDIR**

*+ following interested PPF partners in NY:*

* *Ford Foundation*
* *Apple*