Cybersecurity Tech Accord Feedback on the Pall Mall Process – Code of Practice for States to Tackle the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities (CCICs)

On behalf of the Cybersecurity Tech Accord, I am writing to submit the Tech Accord's feedback on the Pall Mall Process Code of Practice for States. Launched in 2018, the Cybersecurity Tech Accord is a coalition of over 155 technology companies serving as the voice of the tech industry on matters of peace and security online. Our signatories include small and medium-sized technology and cybersecurity enterprises, as well as global technology companies committed to four foundational principles: strong defense, no offense, improved cybersecurity, and multistakeholder partnerships.

The ongoing proliferation of cyber mercenaries, firms that develop and sell malicious tools and services, largely to governments, has become an area of pressing concern for our coalition. The growth of this market severely undermines security by incentivizing the exploitation of vulnerabilities instead of responsible disclosure. This is why the Cybersecurity Tech Accord has worked to support responsible industry practices to limit cyber mercenary operations, and began tracking government-led efforts to start placing meaningful boundaries on the cyber mercenary market itself. The Tech Accord has been closely following the Pall Mall process as part of our longstanding engagement in multi-stakeholder initiatives that aim to push back against cyber mercenaries. Our initiative was part of the Paris Call working group that released the Paris Call Blueprint on Cyber Mercenaries at the Paris Peace Forum in 2023.

We are grateful for the opportunity to contribute to the Pall Mall Process and provide feedback on the draft Code of Practice for States. **Our key recommendations, focused on Pillar 3 – Oversight and Pillar 4 – Transparency, are aimed at making the provisions around oversight and transparency as effective as possible.**

Regarding **Pillar 3** on oversight, we recommend including provisions that aim to ensure that the structures set up for oversight are effective, by regularly reviewing their activity and ensuring their independence and impartiality. In addition, we recommend including provisions that ask states to allocate enough resources to ensure these oversight structures are staffed with cybersecurity professionals and technical experts trained to understand the workings of CCICs. The Code should also encourage states to set up mechanisms for reviewing the government use of CCICs through judicial or other independent and impartial authorities, and to collect technical data on the usage of CCIC in malicious incidents in a standardized format that can facilitate information sharing.

Lastly, we would recommend including provisions that encourage states to develop a shared methodology for attributing CCIC incidents.

Regarding **Pillar 4** on transparency, we recommend that the Code includes provisions asking states to work towards developing a standardized format for reporting to support robust information sharing between governments. The Code could also ask states to set up whistleblower programs to make sure that the vulnerabilities that CCIC's use are procured legally. In addition, states could be encouraged to keep a record of incidents involving the use of CCICs, including details such as the tools used, the nature of the intrusion, and the impact on the target. States could also be encouraged to create a system to report CCICs to affected targets, companies or individuals.

Lastly, given the global reach of this challenge, we recommend including provisions encouraging states leading on this globally to amplify capacity building efforts so as to strengthen the capacity of states whose capabilities may be less developed in the area of tackling CCICs. This would support a more coherent and consistent approach on CCICs at a global level.

Thank you for your consideration. If you require additional information, please get in contact at eravaioli@apcoworldwide.com.

Sincerely,

Edoardo Ravaioli

Head of Secretariat, Cybersecurity Tech Accord