A Unified Front Against Cyber Mercenaries

precisionpconline.com/a-unified-front-against-cyber-mercenaries/

November 11, 2023

Multistakeholder commitments from the Paris Call community

The Cybersecurity Tech Accord welcomes the new *Paris Call Blueprint on Cyber Mercenaries* released today by the Paris Peace Forum and developed by a coalition within the Paris Call for Trust and Security in Cyberspace. The Blueprint aims to drive multistakeholder cooperation to curb the growing market of cyber mercenaries around the world. The recommendations included in the Blueprint build on the industry principles released by the Cybersecurity Tech Accord last spring and go a step further to underscore that this challenge requires multistakeholder cooperation. The Cybersecurity Tech Accord has been a supporter of the Paris Call since its launch in 2018 and is proud to have joined the working group responsible for this new guidance. Preventing harms from firms that weaponize peaceful technology for profit will take industry action, as well as support from civil society; but perhaps more than anything it will require initiative and leadership by governments. That is why, as we welcome this new guidance today, we are also announcing that the Cybersecurity Tech Accord will intend to track and highlight which governments adopt policies consistent with these recommendations moving forward.

A growing and dynamic threat

The term “cyber mercenaries” refers to private entities operating in a grey market for the development of offensive cyber capabilities generally sold to government customers. The malicious tools and services sold by these firms constitute some of the most sophisticated threats and largest contributors to cyber risk across the digital ecosystem. The existence of this market incentivizes the widespread development of military-grade cyber weapons that target consumer products and inevitably proliferate to a wide range of actors. Moreover, especially in the hands of more authoritarian states, these capabilities have been used to target, track and surveil political dissidents, journalists and human rights defenders around the world.

The persistence of the cyber mercenary market is antithetical to the principles of the Paris Call. It is fitting then that a working group including governments, companies and civil society brought together by the Paris Call are today announcing the below recommendations for respective stakeholders seeking to limit the risks posed by cyber mercenaries. Each of these recommendations is expanded upon in further detail in the statement from the working group, which the Cybersecurity Tech Accord was proud to have participated in.

Priority recommendations from Paris Call working group

Government recommendations

- Develop clear acceptable use guidelines
- Safeguard ICT exports from malicious use
- Adopt transparent procurement practices
- Mandate vendor verification
- Blacklist violators

Government and industry recommendations

- Prevent purchases by non-State actors
- Require oversight

Industry recommendations

- Respect the Cybersecurity Tech Accord industry principles
- Vulnerability discovery and handling

Industry and civil society recommendations

Publish evidence-based findings to contextualize threats

Civil society recommendations

Expand collective knowledge of the market

Government accountability tracking

Looking at the list of recommendations above, governments clearly have a large role to play in setting expectations and promoting accountability when it comes to their procurement and use of cyber mercenaries. The unrestricted use, and too-often abuse, of such firm's services is inconsistent with the values of liberal democracies in particular. To this end, the Cybersecurity Tech Accord is announcing today that we will begin tracking which governments – starting with those who have endorsed the Paris Call – adopt policies and regulations to live-up to the guidance reflected in the first seven recommendations in bullet points above (on the left). This is intended to help showcase responsible practices and different approaches that may inspire similar steps to be taken by other governments to address a shared problem.

The Cybersecurity will launch this tracker based on the guidance for governments in advance of the Summit for Democracy in March, 2024, as the next prominent gathering of the world's democracies focused on addressing these challenges. For examples of recent government actions reflect this guidance and help limit the risk posed by cyber mercenaries, we would like to highlight the following initiatives and resources.

- **European Union:** PEGA Committee final report recommendations (June 2023)
- **United States:** Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security (March 2023)
- **Freedom Online Coalition:** Guiding Principles on Government Use of Surveillance Technologies (March 2023)
- **France and the United Kingdom:** UK-France Joint Leaders' Declaration (March 2023)
- **Government coalition:** Declaration for the Future of the Internet (March 2022)

While much of the activity above focuses on the use of spyware technology developed by cyber mercenary firms for surveillance, the threats posed by independent companies developing malicious software certainly goes much further than and we encourage governments to take a more expansive view of the issue space.

Industry stepping up

For our part, the Cybersecurity Tech Accord continues to encourage the tech sector to take actions, as able, to counter cyber mercenaries across our respective platforms and consistent with the principles we released last spring. Recent examples of industry action against cyber mercenaries includes the following:

- **Rooting out spyware (Bitdefender)** – Earlier this year, Bitdefender discovered and reported on a spyware delivered surreptitiously via VPN installers, identifying indicators of infection. The spyware, SecondEye, was developed by a legitimate company based in Iran and was being used to surveil targets seeking to use VPN services in a region where they are widely utilized to avoid government internet controls. Most of these detections originated from Iran, with a small pool of victims in Germany and the US as well.
- **Concrete Industry Regulatory Principles (Meta)** – Building on successive threat reports providing insights into the spyware industry and its indiscriminate targeting of people, Meta released its comprehensive recommendations and regulatory principles for addressing these growing threats.
- **Blue Tsunami takedown (Microsoft/LinkedIn)** – LinkedIn, supported by Microsoft Threat Intelligence, recently shutdown hundreds of likely fake accounts and dozens of fake company pages on the LinkedIn platform that were linked to a cyber mercenary group "Blue Tsunami." This actor engages in social engineering to facilitate human intelligence collection. Microsoft assesses with high confidence that Blue Tsunami activity is strongly associated with Black Cube, a private intelligence firm. Blue Tsunami is known to primarily target individuals of interest to Black Cube clients worldwide, including those who work in human rights, financial, and consulting industries, among many others.

- **Podcast: Cyber mercenaries and the global surveillance-for-hire market (Cybersecurity Tech Accord)** – The topic of cyber mercenaries was discussed at length in a recent episode of the *Patching the System Podcast* featuring representatives from Cisco and the CyberPeace Institute drawing greater attention to the phenomenon and the types of legal, administrative, and technical actions are being taken in response by industry and other actors.

The rise of cyber mercenaries poses a serious threat to human rights, democracy, and peace in the digital age. In the face of this challenge it is encouraging to see the emergence of such widespread consensus around not only the urgency of the issue but also the responsibilities of different stakeholders for addressing it. The Paris Call guidance released today gives hope for more a more coordinated and effective response from governments, civil society, and the private sector. The Cybersecurity Tech Accord looks forward to continuing to support these efforts.

The post A Unified Front Against Cyber Mercenaries appeared first on Cybersecurity Tech Accord.