hackerone

March 6, 2025

VIA ELECTRONIC SUBMISSION
initiatives.dgp-asd-cyber@diplomatie.gouv.fr
pallmallprocess@fcdo.gov.uk

Re: Pall Mall Process Draft Code of Practice for States to Tackle the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities

Dear Sir or Madam,

HackerOne Inc. (HackerOne) submits the following comments in response to the Pall Mall Process's Draft Code of Practice for States on Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities (CCICs).[1] We commend the UK and France for their leadership in advancing this critical work.

As commercial spyware and offensive cyber tools continue to proliferate and are increasingly misused, the global community has a shared responsibility to take action to manage these capabilities. The misuse of such tools can cause significant harm to individuals, organizations, and nations. Therefore, it is imperative that governments establish and follow clear guidelines that prioritize security, accountability, and human rights. While we recognize and appreciate the efforts made to incorporate our previous feedback, we believe additional considerations should be incorporated into the Code of Practice for States to further enhance its impact and effectiveness.

HackerOne is the global leader in human-powered security, harnessing the creativity of the world's largest community of security researchers with cutting-edge AI to protect digital assets. The HackerOne Platform combines the expertise of our elite community and the most up-to-date vulnerability database to pinpoint critical security flaws across your attack surface. Our integrated solutions, including bug bounty, pentesting, code security audits, spot checks, and AI red teaming, ensure continuous vulnerability discovery and management throughout the software development lifecycle. HackerOne has helped find and fix vulnerabilities for sector leaders including Coinbase, General Motors, GitHub, Goldman Sachs, the Financial Times, Starling Bank, the U.S Department of Defense, and the UK Ministry of Defence.

In support of mitigating harm from and promoting responsible use of CCICs, we offer the following remarks and recommendations:

Section 1 - Preface

We appreciate the Pall Mall Process's early recognition of the value of vulnerability disclosure, bug bounties, penetration testing, and good-faith cybersecurity research within the

[1] Pall Mall Process, Draft Code of Practice for States.

Code of Practice.[2] By fostering a culture of transparency, collaboration, and continuous improvement, these activities help identify and mitigate vulnerabilities before they can be exploited. The inclusion of such practices reflects a forward-thinking approach to cybersecurity and sets a positive example for governments to prioritize proactive security measures.

Section 2 – Voluntary Good Practice for States

Pillar 3 - Oversight

We seek clarification regarding the proposal in Section 2 – Voluntary Good Practice for States, Pillar 3 - Oversight, specifically 9.b.i, which suggests controls for researchers contracting with governments. It is essential to clarify whether these "controls" are intended as restrictive measures or as guidelines.

As currently drafted, HackerOne disagrees with the idea of imposing restrictive controls on researchers contracting with governments. While preventing the irresponsible use of cyber intrusion capabilities is crucial, imposing undue restrictions on legitimate security research would hinder efforts to enhance cybersecurity. Security researchers play a critical role in identifying and addressing vulnerabilities, and unnecessary constraints could stifle innovation, create a chilling effect, and hinder timely responses to emerging threats.

Instead of restrictive controls, we recommend that governments implement clear, comprehensive guidelines for security researchers. These guidelines should define ethical conduct and best practices which outline permissible activities, the systems covered, and expectations for responsible behavior. Clear frameworks will help ensure that researchers understand their boundaries. Governments should also provide transparency by defining how vulnerabilities should be reported, specify timelines, and offer incentives for responsible disclosure. Easily accessible channels should be available to facilitate rapid reporting.

We also respectfully disagree with 9.b.ii, which suggests implementation of mechanisms for limiting the ability of cybersecurity professionals with expertise in deploying CCICs from using their offensive cyber skills for malicious purposes after leaving government service. While concerns about the potential misuse of such expertise are valid, there is significant risk that such mechanisms may inadvertently be over-inclusive and result in ambiguity that discourages skilled professionals from beneficial contributions to cybersecurity.

Pillar 4 – Transparency:

We strongly support 10.a.ii, which advocates for better support and protection for the commercial and civil society cyber threat researcher ecosystem. However, we urge Pall Mall Process stakeholders to advocate for legal protections for security researchers, which remains a critical issue that has not been adequately addressed. Many researchers face legal uncertainty when conducting security research, even when acting responsibly and in good faith. The lack of

[2] Id, pg. 3.

clear legal distinctions between ethical cybersecurity practices, cybercrimes, and unauthorized access puts researchers in precarious positions and can discourage critical research.

To address this, we recommend that governments establish well-defined safe harbors for good-faith security research and amend their computer crime laws accordingly. We encourage states to follow the example set by the U.S. Department of Justice, which established a charging policy under the Computer Fraud and Abuse Act (CFAA) to differentiate between malicious activities and responsible security research. This policy directs federal prosecutors to decline prosecution of researchers acting in good faith.[3]

In addition, we agree with proposal 10.b.i, which notes that states should define an evaluation process for decisions surrounding discovered cybersecurity vulnerabilities. Every government agency should have a clear, structured process in place to evaluate and prioritize vulnerabilities as they are discovered. This will ensure that high-risk vulnerabilities are addressed promptly, reducing the likelihood of exploitation.

Finally, we are very heartened to see that Pall Mall Process stakeholders accepted our recommendation to encourage commercial entities to establish and publish their own Vulnerability Disclosure Programs as a way to mitigate vulnerabilities. This is a significant step toward fostering a more transparent and responsible cybersecurity ecosystem, and we applaud the Pall Mall Process for recognizing the importance of these practices.

* * *

HackerOne appreciates the opportunity to provide a response to this process. As the conversation around this topic continues to evolve, we welcome the opportunity to further serve as a resource and provide insights on ways to curb the misuse of cyber intrusion capabilities.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne

[3] U.S. Dept. of Justice, Charging Policy - 9-48.000 Computer Fraud And Abuse Act, May 19, 2022, https://www.justice.gov/media/1223666/dl?inline