Pall Mall Process

6-7 FEBRUARY 2024

THE PALL MALL PROCESS: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities

Lancaster House, London, 6 February 2024

We, as participant representatives of States, international organisations, private industry, academia, and civil society met to participate in an international conference hosted by the United Kingdom and France. The conference discussed the challenges posed by the proliferation and irresponsible use of commercial cyber intrusion capabilities and initiated the Pall Mall Process.

1. In acknowledgment of the need for greater international action and multi-stakeholder consultation on this issue, while recognising the need for legitimate and responsible development and use of cyber intrusion capabilities, we resolve to initiate an inclusive global process – the Pall Mall Process. The Pall Mall Process will establish guiding principles and highlight policy options for States, industry and civil society in relation to the development, facilitation, purchase, and use of commercially available cyber intrusion capabilities. This Process builds on the whole of society approach to cyberspace and acknowledges the importance of public-private partnership and multi-stakeholder collaboration in the pursuit of a more secure cyberspace.

2. The growing commercial market enabling the development, facilitation, purchase, and use of commercially available cyber intrusion capabilities raises questions and concerns over its impact on national security, human rights and fundamental freedoms, international peace and security, and a free, open, peaceful, stable, and secure cyberspace.

3. With its transformational impact on the cyber landscape, this growing market vastly expands the potential pool of state and non-state actors with access to commercially available cyber intrusion capabilities and increases the opportunity for malicious and irresponsible use, making it more difficult to mitigate and defend against the threats they pose. These threats, including to cyber stability, human rights, national security, and digital security at large, are expected to increase over the coming years.

4. Without international and meaningful multi-stakeholder action, the growth, diversification, and insufficient oversight of this market raises the likelihood of increased targeting for profit, or to compromise a wider range of targets, including journalists, activists, human rights defenders, and government officials. It also risks facilitating the spread of potentially destructive or disruptive cyber capabilities to a wider range of actors, including cyber criminals. Uncontrolled dissemination may increase the breadth of access to sophisticated capabilities

and, as a consequence, the complexity of incidents for cyber defence to detect and mitigate. This trend risks contributing to unintentional escalation in cyberspace.

5. The market encompasses a wide variety of products and services that are continually evolving and diversifying. The market includes an interconnected ecosystem of researchers, developers, brokers, resellers, investors, corporate entities, operators, and customers. To aid discussions on the threats posed and potential risks, we offer some working definitions at **Annex A**.

6. We recognise that, across the breadth of this market, many of these tools and services can be used for legitimate purposes, but they should not be developed or used in ways that threaten the stability of cyberspace or human rights and fundamental freedoms, or in a manner inconsistent with applicable international law, including international humanitarian law and international human rights law. Nor should they be used without appropriate safeguards and oversight in place. We resolve to explore the parameters of both legitimate and responsible use, by State, civil society, legitimate cyber security, and industry actors alike, throughout the Pall Mall Process.

7. We recall that existing international law applies to the conduct of States in cyberspace and that all UN Member States have committed to act in accordance with the framework for responsible state behaviour in cyberspace. We reaffirm that States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, should respect human rights, and should encourage responsible reporting of ICT vulnerabilities, consistent with norms 13(e), (i) and, (j) from the 2015 and 2021 UN GGE Reports on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, subsequently endorsed by consensus by the UN General Assembly.

8. In addition, we encourage the private sector to respect and support human rights, including as set out in the United Nations Guiding Principles on Business and Human Rights. All actors, including both States and the private sector, should seek to ensure that the development, facilitation, purchase, export, and use of commercially available cyber intrusion capabilities does not undermine stability or threaten human rights and fundamental freedoms, including in cyberspace. We encourage the multi-stakeholder community to continue improving its awareness and efforts to prevent commercially available cyber intrusion capabilities from being used irresponsibly.

9. Recognising the importance of cyber capacity building, and the necessity of cyber resilience in preparing, mitigating, responding, recovering, and learning from destructive or disruptive cyber attacks, we strongly encourage States, industry, civil society, academia, members of the technical community, and individuals to continue to build greater global cyber capacity for defensive purposes to ensure secure, safe, inclusive, and trustworthy access to the opportunities offered by digital technologies. We acknowledge the benefit that good faith security research, vulnerability disclosure, bug bounties for cyber defensive purposes and penetration testing can have on cyber security defences.

We recognise the vital role that industry plays in strengthening cyber security and supporting victims in responding to malicious cyber activity.

10. We welcome existing efforts by States to take steps to tackle the issue, including efforts made via existing international export control frameworks and the ongoing development of domestic action by national jurisdictions. We recognise civil society and industry efforts which have increased global awareness on this issue including critical investigations, reporting, and support to victims.

11. In the context of future multi-stakeholder cooperation, and to inform the Pall Mall Process, we consider the following pillars helpful to frame our future engagement involving States, industry, civil society, and academia representatives:

11.1. **Accountability** – Activity should be conducted in a legal and responsible manner, in line with the framework for responsible state behaviour in cyberspace and existing international law, and domestic frameworks. Actions should be taken, as appropriate, to hold States accountable whose activity is inconsistent with international human rights law and to hold non-state actors to account in domestic systems, as appropriate.

11.2. **Precision** – The development and use of capabilities should be conducted with precision, in such a way as to ensure they avoid or mitigate unintended, illegal, or irresponsible consequences.

11.3. **Oversight** – Assessment and due diligence mechanisms (by both users and vendors – including States and industry actors) should be in place to ensure activity is carried out legally, responsibly, and may incorporate principles such as lawfulness, necessity, proportionality, and reasonableness, informed by existing international law and norms.

11.4. **Transparency** – Business interactions should be conducted in such a way as to ensure that industry and users understand their supply chains; building trust and confidence in the responsible business practices of vendors they interact with.

12. Following our participation at today's discussions, we resolve to engage in an ongoing and globally inclusive dialogue, complementary to other multilateral initiatives, and look forward to advancing this process in the coming months. A follow-up conference will be organized in France in 2025 to take stock of the progress made under this agenda and bring forward further discussions.

States and international organisations represented:

African Union

Australia

Belgium

Canada

Czechia

Denmark

Estonia

Finland

France

Germany

Greece

Gulf Cooperation Council

Italy

Japan

Malaysia

New Zealand

Norway

Poland

Republic of Cyprus

Republic of Ireland

Republic of Korea

Romania

Singapore

Sweden

Switzerland

United Kingdom of Great Britain and Northern Ireland

United States of America

Industry represented:

BAE Systems Digital Intelligence

ESET

European Cyber Conflict Research Incubator CIC

Google

HackerOne

Luta Security

Margin Research

MDSec

Meta

Microsoft

NCC Group

NextJenSecurity

Sekoia.io

YesWeHack

Civil society and academia represented:

Alejandro Pisanty

Allison Pytlak, Stimson Center

Atlantic Council

CyberPeace Institute

Gefona Digital Foundation

GEODE (French Institute of Geopolitics, University Paris 8)

ICT4Peace

Professor Nnenna Ifeanyi-Ajufo, Leeds Beckett University

Paris Peace Forum

Royal Holloway, University of London

Royal United Services Institute

Shadowserver Foundation

ANNEX A: Working definitions to aid discussions on commercially available cyber intrusion capabilities

To ground discussions in common language, we offer the below working definitions which cover key aspects of the commercial cyber intrusion market. We note that these definitions are not exhaustive nor definitive and will be shaped throughout the Pall Mall Process. The working definitions employed here are merely for illustrative purposes and are not intended to be comprehensive nor binding.

I. **Commercially available cyber intrusion capabilities** describe tools and services made available by cyber intrusion companies and similar high-end capabilities developed by other companies. Capability providers may also operate based on **as-a-service models** of operation. As-a-service describes a model whereby an entity develops, provides, and supports a capability for a customer. These include, but are not limited to:

   i. **Access-as-a-service** whereby one entity provides the access vector by which end-users are able to gain unauthorised access to computer systems, and;
   ii. **Malware**[1]**-as-a-service** by which providers develop, maintain, and provide malware to be used against targets on behalf of a customer.

II. **Cyber intrusion companies** refers to commercial business entities that offer 'off-the-shelf' products or services for computer system penetration or interference in exchange for commercial benefit. Such entities might include developers or sellers of vulnerabilities and exploits, companies developing and selling cyber intrusion products or companies offering hacker-for-hire services. These include, but are not limited to:

   i. **Hacking-as-a-service companies**, which are companies providing the capability and often the supporting infrastructure for computer system penetration as a service. The customers usually identify requirements, such as target selection and consume the resulting information. This does not include consensual access, such as security testing; and
   ii. **Hackers-for-hire**, which are unaffiliated individuals or groups of actors that are hired by States, entities or even individuals to conduct computer system penetration to meet customer requirements. They use their own tools and techniques and are aware of, and in some cases may select, who they are targeting.

III. **The vulnerability and exploit marketplace** describes the commercial trade in zero-day vulnerabilities and exploits[2] that enable cyber intrusion. It does not refer

[1] **Malware** is derived from 'malicious software', and includes viruses, trojans, worms or any code or content used for illicit purposes against computer systems, networks or devices.

[2] A **vulnerability** is a weakness, or flaw, in a system or process. An attacker may seek to exploit a vulnerability to gain access to a system. The code developed to do this is known as an **exploit**. A **zero-day** exploit exploits a vulnerability where there are no security fixes yet available. A zero-day vulnerability becomes an **n-day** vulnerability once a security fix (patch) has been issued by the vendor. Exploitation of an n-day vulnerability relies on finding systems that have not been updated.

to the commercial payment for vulnerability research to enable cyber defence, such as security testing, or bug bounty programs for cyber defensive purposes.

IV. **Commercial intrusive surveillance software,** sometimes referred to as 'spyware', describes commercially-available software and tools that provides the user the capability to gain remote access to a computer system, without the consent of the user, administrator, or owner of the computer system, in order to access, collect, exploit, extract, intercept, retrieve, alter or delete or transmit content, including information stored on or transmitted through a device connected to the Internet. This may include the capability to record video, audio or calls, or to track the location of the computer.

V. **Destructive or disruptive cyber capability** refers to capability developed to enable a damaging effect through cyber means on a computer system. This might include tools designed to enable intrusion and interference in operational technology, such as ransomware or wipers.