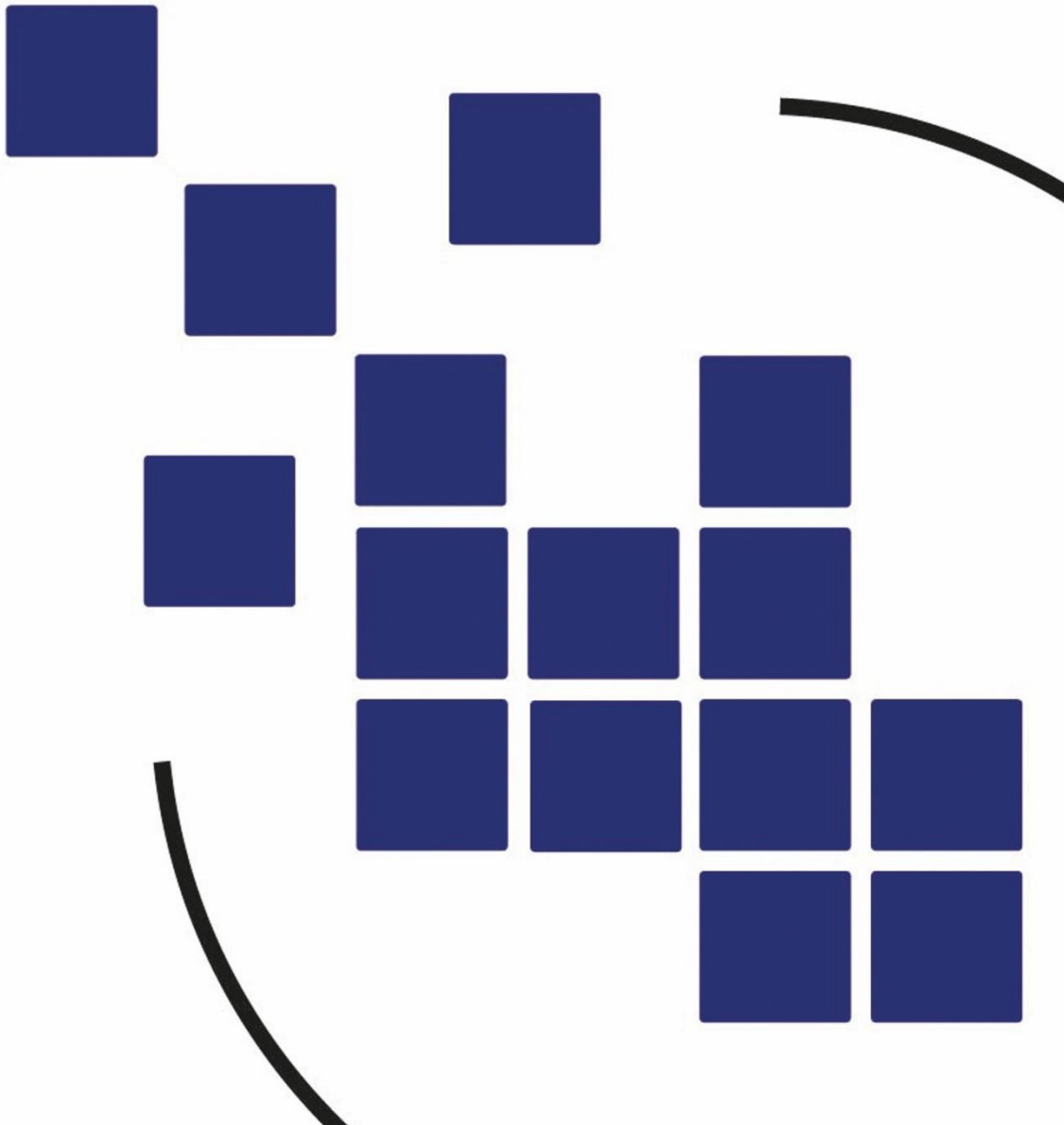
PALL MALL PROCESS

CODE OF PRACTICES FOR STATES

To tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities



Section 1 - Preface

1. We as States and international organisations support this voluntary and non-binding 'Code of Practice' for States, through which to tackle the challenges posed by the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICs).

2. The Pall Mall Process is an iterative multistakeholder initiative launched in 2024 to respond to these challenges. It intends to bring together States, international organisations, private industry, academia and civil society to establish guiding principles and highlight policy options in relation to the development, facilitation, purchase, transfer and use of CCICs. As supporters of this Code of Practice, we recognise:

2.a. Many of these tools and services can be developed or used for legitimate purposes. However, the proliferation of CCICs raises questions and concerns over the impact of their potential irresponsible use on national security, respect for human rights and fundamental freedoms, international peace and security, and an open, secure, stable, accessible, peaceful and interoperable cyberspace.

2.a.i. For the purposes of the Pall Mall Process, **irresponsible use** by State or non-State actors should be understood as use in ways that threaten security, respect for human rights and fundamental freedoms or the stability of cyberspace, without appropriate safeguards and oversight in place or in a manner inconsistent with applicable international law or the consensus United Nations framework on responsible State behaviour in cyberspace, with due regard to domestic law where relevant. Moreover, CCICs should not be used to target individuals or members of a group based on any discriminatory grounds, to violate or abuse human rights and fundamental freedoms, including the right to freedom of expression, and that no one should be subjected to arbitrary or unlawful interference with privacy.

2.a.ii For the purposes of the Pall Mall Process, **proliferation** should be understood as the uncontrolled dissemination of CCICs to state and non-state actors in a manner that significantly increases the breadth of access to these tools and services and potential for their irresponsible use.

2.b. The market for CCICs encompasses a wide variety of cyber intrusion companies offering 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, including States. The emergence of new technologies such as artificial intelligence, although they can enhance cyber defensive capabilities including the detection, response and remediation of malicious cyber incidents, are likely to increase the availability of cyber intrusion tools and services and the threat stemming from their irresponsible use, whilst making them more difficult to monitor and regulate.

2.c. This growing market vastly expands the potential pool of state and non-state actors with access to CCICs and increases the opportunity for irresponsible use, making it more difficult to mitigate and defend against the threats they pose. These threats, including to security, respect for human rights and fundamental freedoms and the stability of cyberspace, are expected to increase over the coming years.

2.d. Without international and meaningful multistakeholder action, the growth, diversification, and insufficient oversight across this market raises the likelihood of increased irresponsible targeting of a range of public and private targets, including journalists, human rights defenders and government officials, as well as critical national infrastructure. It also risks facilitating the spread of potentially destructive or disruptive cyber capabilities to a wider range of actors, including cyber criminals. Increasing access to sophisticated capabilities may expand the complexity of incidents and opportunities for irresponsible use, and could contribute to unanticipated risks arising from the

interaction of multiple actors in cyberspace, including potential unintentional escalation in cyberspace.

3. We recall that all United Nations Member States have affirmed by consensus that international law, including customary international law and the principles of sovereignty and non-intervention, apply to the conduct of States in cyberspace, including in the context of States' regulation and use of CCICs. The pertinent international legal frameworks where applicable in relation to States' regulation of the development, transfer and use of CCICs include, but are not limited to:

- 3.a. The United Nations Charter;

- 3.b. International human rights law, including but not limited to the right to freedom of thought, conscience and religion, the right to freedom of opinion, the right to freedom of expression, the right of peaceful assembly with others, the right to freedom of association, and that no one should be subjected to arbitrary or unlawful interference with his privacy, as set out in the International Covenant on Civil and Political Rights and other applicable international and regional treaties;

- 3.c. International treaties, alongside other applicable regional conventions;

- 3.d. International humanitarian law, with respect to cyber activities carried out with CCICs in the context of an armed conflict.

4. We further recall that all United Nations Member States have committed to act in accordance with the consensus United Nations framework on responsible State behaviour in cyberspace, which relies on applicable international law and additional voluntary and non-binding norms of responsible behaviour. We reaffirm that States should seek to prevent the proliferation of malicious Information Communications Technology (ICT) tools and techniques and the use of harmful hidden functions, should respect and protect human rights, and should encourage coordinated reporting of ICT vulnerabilities, and should not knowingly allow their territory to be used for inter-nationally wrongful acts using ICTs, consistent with the voluntary and non-binding norms 13 (c), (d), (e), (i) and, (j) from the 2015 and 2021 United Nations Group of Governmental Experts (GGE) Reports on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, subsequently endorsed by consensus by the United Nations General Assembly (UNGA), and most recently the 2024 Open-Ended Working Group (OEWG) Annual Progress Report. We further recall other pertinent UNGA resolutions, including Resolution 217 adopting the Universal Declaration of Human Rights, Resolution 79/175 on the right to privacy in the digital age, Resolution 78/213 on the promotion and protection of human rights in the context of digital technologies, and other pertinent Human Rights Council resolutions, including Resolution 57/29 on the promotion, protection and enjoyment of human rights on the Internet and new and emerging digital technologies and human rights 47/23.

5. The actions foreseen under this document sit alongside our common objective to close all digital divides. We recognise the role confidence building measures can play to enable information sharing to address this issue, the importance of cooperation on cyber capacity building, and the necessity of cyber resilience in identifying, preparing, mitigating, responding, recovering, and learning from destructive or disruptive malicious cyber activities. 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, in line with the cyber capacity building principles set forth in the 2021 OEWG Final Substantive Report.

6. We recognise the vital role that industry plays in strengthening cyber security and supporting victims and Governments in responding to and recovering from malicious cyber incidents. We acknowledge the benefit that security by design policies, good faith cyber security research, coordinated vulnerability disclosure, and penetration testing can have on cyber security and national resilience. We further recall that the United Nations Guiding Principles on Business and Human Rights sets out that States have a duty to protect human

rights, that business enterprises have a responsibility to respect human rights, and that States must take appropriate steps to ensure that when business-related human rights abuses occur within their territory and/or jurisdiction, those affected have access to effective remedy, including during the development, facilitation, purchase, transfer and use of CCICs.

Section 2 – Voluntary Good Practice for States

7. In line with our common objective to uphold our international legal obligations and promote responsible state behaviour, we intend to take domestic and international action to tackle this issue. This voluntary and non-binding 'Code of Practice' establishes practices for States in relation to the development, facilitation, purchase, transfer and use of CCICs, subject to national legal frameworks and the inherent limitations of national jurisdictions and where applicable to particular capabilities, through the four pillars underpinning the Pall Mall Process, the guiding principles of: accountability, precision, oversight and transparency.

8. **Pillar 1 - Accountability:** Activity should be conducted in a lawful and responsible manner, in line with existing applicable international law, the consensus United Nations framework on responsible State behaviour in cyberspace, and domestic legal frameworks. Actions should be taken, as appropriate, to promote international adherence to this Code of Practice and address irresponsible activity inconsistent with applicable international law (including international human rights law) and domestic legal systems, as appropriate. To this end, we will commit to:

- 8.a. Establishing or applying national frameworks to the extent possible in relation to the development, facilitation, purchase, transfer, and use of CCICs. Practices include:

    8.a.i. Ensuring, through an appropriate system of rules, regulations and oversight, that any development, facilitation, purchase, transfer, and use of CCICs is carried out responsibly, and solely for lawful, legitimate and necessary purposes. Any such framework should respect applicable international law, including international human rights law, and the consensus United Nations framework on responsible States behaviour in cyberspace.

- 8.b. Applying controls, where applicable, on the export of CCICs to mitigate risks of potential irresponsible use. Practices include, where applicable and as appropriate:

    8.b.i. Ensuring export control licensing decisions concerning CCICs take into account the risk, among others, of their use in connection with internal repression, as appropriate, and/or the commission of serious violations or abuses of human rights;

    8.b.ii. Ensuring licencing decisions limit the export of CCICs to a specific end-user and for a defined lawful and legitimate purpose, and where consideration of these elements does not raise concerns regarding lawful and responsible use or the risk of diversion, recognising that such controls should not be used to impose undue market restrictions to States, or to hinder legitimate cybersecurity activity;

    8.b.iii. Reviewing, and where necessary preparing, published guidance to ensure it clarifies where and how States existing domestic export control regulations place obligations on exporters, including the consequences of non-compliance with these obligations;

    8.b.iv. Exploring opportunities to update multilateral or domestic export control regimes to ensure appropriate coverage of CCICs;

    8.b.v. Exploring opportunities for needs-based capacity building support to address the technical challenges presented by the implementation and enforcement of controls.

- 8.c. Incentivising responsible activity across the market for CCICs. Practices include:

8.c.i. Assessing vendors to Governments with regards to national and international cybersecurity standards and respect for the rule of law and applicable international law, including human rights and fundamental freedoms, as well the United Nations Guiding Principles on Business and Human Rights;

8.c.ii. Exploring opportunities to align procurement controls across government, as appropriate, and defining which entities under their jurisdiction are authorised to, import, purchase, hold, offer, sell, rent and use CCICs and in what capacity;

8.c.iii. Exploring opportunities to establish or enhance formal processes to debar or exclude potential CCIC vendors that do not meet the standard of responsible behaviour from Government procurement, to send a clear message to industry that illegal or irresponsible activity is unacceptable;

8.c.iv Exploring opportunities to encourage CCIC vendors to conduct human rights due diligence, in order to identify, prevent and mitigate their adverse human rights impacts.

- 8.d. Developing a toolkit of measures, including the use of existing policy tools, through which to deter irresponsible behaviour across the global market for CCICs and consider how they should be used. Practices include:

  8.d.i. Identifying policy levers to target and impose a cost, where appropriate and in compliance with due legal process, on specific individuals and entities involved in carrying out, facilitating, or benefiting from the irresponsible use of CCICs, such as criminal proceedings, financial or travel restrictions;

  8.d.ii. Exploring opportunities to cooperate with each other and industry partners on the use of such measures, in order to maximise their impact and send a strong signal that illegal or irresponsible activity is unacceptable;

  8.d.iii. Collaborating when appropriate with international and industry partners to act against the development, purchase, facilitation, transfer of CCICs to and use of CCICs by irresponsible and illegitimate non-state actors, such as criminals.

- 8.e. Providing support for victims targeted or affected by the irresponsible use of CCICs. Practices include:

  8.e.i. Where necessary, providing procedures for those claiming redress as a result of the irresponsible use of CCICs, including ensuring access to effective judicial or non-judicial remedies, and, where relevant and appropriate, strengthening cross-border collaboration on CCIC investigations;

  8.e.ii. Carrying out awareness-raising and provide cybersecurity advice to those at high risk of being targeted through irresponsible use of CCICs, such as journalists, human rights defenders and government officials;

  8.e.iii. Improving support to victims affected by the irresponsible use of CCICs;

  8.e.iv. Exploring opportunities to establish and strengthen reporting mechanisms through which individuals or groups can raise concerns about irresponsible use of CCICs.

9. **Pillar 2 – Precision:** The development, facilitation, purchase, transfer and use of CCICs should be conducted with precision, in such a way as to ensure they avoid irresponsible use or mitigate the consequences of it. To this end, we will commit to:

- 9.a. Developing, and where relevant articulating policy surrounding Government use of CCICs. Practices include:

  9.a.i. Preparing, where relevant, a national position on responsible Government use of CCICs;

  9.a.ii. Ensuring that their use of CCICs does not violate human rights and fundamental freedoms;

  9.a.iii. Limiting the use of CCICs to where necessary for lawful purposes, such as in the context of legal frameworks pertaining to national security and defence, or the investigation and prevention of serious crime or for cybersecurity activities;

  9.a.iv. Ensuring that decisions to use CCICs are tested and the design of operations to deploy them are based on nationally determined principles, examples of which could include 'proportionality, subsidiarity, necessity, non-discrimination, time limitation, and security';

  9.a.v. Establishing or defining clear national policies on what constitutes legitimate use of CCICs in the context of cybersecurity (for example for penetration testing, red teaming and in relation to coordinated vulnerability disclosure policies and bug bounty programmes) and research for cybersecurity activities, aligned to existing protections or safeguards for cybersecurity researchers.

- 9.b. Enhancing internal cross-government information sharing on CCICs. Practices include:

  9.b.i. Encouraging all relevant parts of Government to pool knowledge and understanding of the risks surrounding CCICs and their use, in order to establish a nationally shared view;

  9.b.ii. Exploring opportunities to bring together relevant Government users of CCICs to share responsible and risk-minimising practices, where the distribution of authority within Government allows it;

  9.b.iii. Educating policy makers on the responsible use of CCICs and the procedures for reporting irresponsible activity.

- 9.c. Cooperating between States to incentivise good practice in the use of CCICs. Practices include:

  9.c.i. Exploring opportunities to share examples of domestic good practice internationally to reduce inconsistencies between national approaches towards CCICs, in order to discourage strategic relocation by irresponsible actors;

  9.c.ii. Exploring opportunities for how inter-regional and multilateral cyber capacity building, where appropriate, can be used as a way of supporting States to achieve 'best practices' with regards to a responsible approach to the market.

  9.c.iii. Encouraging inter-regional and multilateral cyber capacity building efforts, where appropriate, to help strengthen global resilience against irresponsible uses of CCICs;

9.c.iv. Exploring opportunities to ensure to the extent possible that, when engaging in international capacity building, any CCICs purchased to facilitate capacity building of international partners, in the cyber sector or otherwise, are used responsibly;

- 9.d. Supporting cybersecurity education and training relevant for professionals operating across the market for CCICs. Practices include:

  9.d.i. Developing skilled cybersecurity professionals who are equipped and incentivised to identify and tackle emerging threats, uphold respect for human rights and safeguard national interests responsibly;

  9.d.ii. Ensuring that Government cyber professionals deploying CCICs are well-informed of, and regularly trained on the way these tools function and in, the responsible and lawful use of CCICs and their technical capabilities;

  9.d.iii. Raising awareness amongst cybersecurity professionals, including independent security researchers, of the implications of their work and the use of CCICs, to incentivise responsible behaviour across the market;

  9.d.iv. Exploring opportunities to coordinate to ensure efforts to establish best practices and standards for professionals operating across the market for CCICs, including independent security researchers, are coherent internationally.

10. **Pillar 3 – Oversight:** Assessment and due diligence mechanisms should be in place to ensure Government activity is carried out legally, responsibly, and may incorporate principles such as lawfulness, necessity, proportionality, and reasonableness, in accordance with applicable international law and guided by the consensus UN framework on responsible State behaviour in cyberspace, and domestic legal frameworks. To this end, we will commit to:

- 10.a. Establishing or ensuring the effective operation of existing structures to provide, in accordance with domestic legal frameworks and to the extent possible, independent and effective oversight of Government use of CCICs to mitigate the risk of irresponsible use. Practices include:

  10.a.i. Ensuring that a clear decision-making and authorisation process is followed and recorded surrounding Government use of CCICs;

  10.a.ii. Establishing or ensuring the effective operation of existing mechanisms for review of the Government use of CCICs, through a judicial or alternative competent authority – for example an independent authority or a national legislature – with guarantees of independence, impartiality, and effectiveness;

  10.a.iii. Providing, as far as possible, such structures with adequate resourcing and the means to understand the specific technical features of CCICs;

  10.a.iv. Encouraging both Government and private entities involved in the development, facilitation, purchase, transfer and use of CCICs to implement a robust ICT security perimeter, in order to prevent any unintended dissemination of CCICs;

  10.a.v. Exploring opportunities for reporting on oversight and control activities.

- 10.b. Developing measures to minimise the risk that Government professionals' offensive cyber skills will be used for irresponsible purposes after leaving Government service. Practices include:

10.b.i. Exploring opportunities to implement controls for researchers contracting with Governments to ensure their work does not contribute to irresponsible activity across the market for CCICs;

10.b.ii. Exploring opportunities to implement measures to incentivise more responsible activity among cyber security professionals with an expertise in deploying CCICs, as well as measures to deter them from using these skills for irresponsible purposes, without impacting the legitimate use of CCICs in the context of cyber security.

11. **Pillar 4 – Transparency:** Business transactions should be conducted in such a way as to ensure that industry and Government users can take reasonable steps to understand their supply chains and toolkits as far as possible, building trust and confidence in the responsible business practices of vendors they interact with. To this end, we will commit to:

- 11.a. Building understanding of the global CCIC market and how it operates. Practices include:

  11.a.i. Seeking opportunities for robust information sharing, including through confidence building measures, bilateral and multilateral frameworks and collaboration with industry, academia and civil society, on their understanding of the CCIC market, and the changing threat that irresponsible activity may present;

  11.a.ii. Identifying opportunities to better support and protect the commercial, civil society and independent cyber threat researcher ecosystem, including from intimidatory litigation;

  11.a.iii. Encouraging industry, civil society, academia and other relevant parties to continue conducting research into CCICs, their use, technical attributes and effects on human rights and fundamental freedoms as well as international peace and security;

- 11.b. Establishing transparency mechanisms surrounding Governments' engagement with and regulation of the market for CCICs. Practices include:

  11.b.i. Defining an evaluation process for decisions surrounding discovered cybersecurity vulnerabilities;

  11.b.ii. Encouraging commercial entities to establish and publish their own coordinated vulnerability disclosure processes, informed by existing international standards;

  11.b.iii. Exploring, where relevant, opportunities to establish or enhance 'Know Your Vendor' and 'Know Your Customer' requirements for vendors to Governments, to create a more consistent and reliable reporting environment across the market;

  11.b.iv. Exploring opportunities to implement appropriate transparency around the processes implemented for controls on the export, government procurement, and use of CCICs, meeting the interest of individuals and the public to be informed, and the need to prevent the disclosure of information that could impact commercial sensitivity, law enforcement, national security and defence interests, and public safety.

12. Together, through our support for and voluntary implementation of measures identified through this 'Code of Practice' for States, and cooperation through the ongoing Pall Mall Process, we will enhance our efforts to prevent irresponsible activity across the global cyber intrusion market and mitigate the threats presented by the proliferation and irresponsible use of CCICs. We encourage individual States to develop and share additional national actions towards addressing this issue. We intend to regularly review progress

on the implementation of these voluntary good practices and on improving accountability across the market. We resolve to keep this Code of Practice up to date with developments in the threat landscape.

Supporting States:

- Austria
- Denmark
- Estonia
- France
- Germany
- Ghana
- Greece
- Hungary
- Ireland
- Italy
- Japan
- Kosovo
- Luxembourg
- Moldova
- Netherlands
- Poland
- Slovakia
- Slovenia
- Sweden
- Switzerland
- United Kingdom