Pall Mall Process

CONSULTATION ON GOOD PRACTICES
SUMMARY REPORT

Contents

INTRODUCTION

In February 2024, representatives from States, international organisations, private industry, academia, and civil society came together to consider the challenges posed by the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICs) and launched the Pall Mall Process (**Annex A**).

With its transformational impact on the cyber landscape, this growing market (including an interconnected ecosystem of researchers, developers, brokers, resellers, investors, corporate entities, operators, and customers) vastly expands the potential pool of State and non-State actors with access to commercially-available cyber intrusion capabilities. This 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 national security, human rights and fundamental freedoms, international peace and security, and a free, open, peaceful, stable, and secure cyberspace, are expected to increase over the coming years.

The Pall Mall Process is an international multistakeholder initiative with the ambition of establishing guiding principles and highlighting policy options for States, industry and civil society in relation to the development, facilitation, purchase, and use of CCICs – commercial business entities that offer 'off-the-shelf' products or services for computer system penetration or interference in exchange for commercial benefit.

As a first step towards advancing these efforts, in August 2024 the Pall Mall Process launched a *consultation on good practices* through which to tackle this shared threat. Through this consultation we have invited relevant stakeholders (including organisations not present at the inaugural Pall Mall conference in February 2024) to share views in response to a questionnaire (**Annex B**) – to identify existing and potential best practices, as well as possible gaps, for:

- **States** – as regulators and potential customers of the market for CCICs;
- **Industry organisations** – involved in and around the market for CCICs, alongside their wider value chain;
- **Civil Society, experts, and threat researchers** – with relevant expertise on the threat presented by the market for CCICs, and responses to it.

Since August, we have received 73 responses to the consultation, including 21 from States, 31 from private industry, and 21 from academia and civil society, and convened a series of virtual workshops to allow for further input.

These responses considered a) the role of States in setting national and international policy and regulatory frameworks, controlling exports, leveraging procurement power and targeting irresponsible actors; b) the role of the intrusion industry in fostering responsible behaviour, managing vulnerabilities and exploits, suppliers and customers; and c) the role of other key stakeholders, including threat researchers, the victims of misuse of CCICs, and the investor community.

This report summarises responses to the Pall Mall Process *consultation into good practices*, including examples, recommendations and concerns raised by participants in written responses and through virtual workshops. The consultation's purpose has been solely to map existing varied efforts and recommendations on good practice across a range of entities, and includes reference to conflicting perspectives provided by respondents. Participation in this consultation has not represented a formal commitment to the Pall Mall Process, nor membership of the initiative, but rather a voluntary contribution through which to advance efforts carried out under the initiative.

This report does **not** represent the policy of the United Kingdom or France.

REPORT

Observations by Respondents

The incentive structure across the market for CCICs is unbalanced

18 respondents discussed the role that incentives play across the market for CCICs in encouraging irresponsible behaviour by vendors and users, with a lack of transparency and high demand from States driving the sale of products.

- Respondents proposed that Governments represented the main driver of irresponsible activity across the market for CCICs as the primary customers of the vendors (including for vulnerabilities and exploits), incentivising researchers operating within the commercial market. Whilst respondents recognised legitimate uses of CCICs to address challenges, including to combat terrorism and assist law enforcement, State actors have increasingly offered higher prices, incentivising the growth of the industry.

- Respondents encouraged the Pall Mall Process to focus on meaningful regulations to combat the proliferation and misuse of CCICs, highlighting that changes in behaviour would not be possible across industry and the skills ecosystem without a significant proportion of governments cooperating to set and facilitate better practices, using regulatory and procurement powers to better incentivise responsible activity and disincentivise the facilitation of the misuse of CCICs.

- Respondents highlighted that as many governments share legitimate aspirations to acquire advanced cyber capabilities, cyber capacity-building has the potential to frame and support responsible development and use of CCICs.

The market for CCICs needs to be defined and better understood

12 respondents highlighted the need for consistent and specific definitions around the market for CCICs, and what capabilities fall into scope, recognising that a lack of understanding around the vendors selling cyber intrusion capabilities and the entities across their supply chains hinders Government approaches to tackling irresponsible activity, and industry self-regulatory practices.

- Respondents reflected on challenges to understanding the networks of operation across the market for CCICs – making joint action more difficult. Public scrutiny has necessarily focused on high end tools and end-to-end service providers, but the interconnected supply chain that sits beneath it, particularly across vulnerability research and exploit broker markets, is less effectively understood.

- Respondents called for definitions outlining the conditions under which CCICs could be used 'legitimately' and 'responsibly,' to allow for more specific technical proposals on preventing the proliferation and misuse. Some respondents raised concerns that discussions around 'general principles' for responsible activity without defined industry terms would be ineffective; suggesting that 'legitimate use' should already be defined through international human rights law.

- Respondents noted the need for a cross-border perspective – with legitimately developed capabilities being re-purposed in some contexts for illicit activities. Respondents highlighted the complementary role that civil society can play here in understanding the State-industry dynamic and bringing additional expertise to support defining incentives and regulations.

- Some respondents further highlighted concerns around the term 'proliferation' placing wholly negative connotations on the market for CCICs, minimising the potential positive contributions of these capabilities to address some challenges.

There is a need for policy consistency, balanced against technology and market shifts

10 respondents discussed the importance of balancing a) the need to ensure that efforts to address irresponsible activity across the market for CCICs through the Pall Mall Process remain dynamic, to allow for an evolving understanding of products and technologies driving irresponsible activity; and b) at the same time providing sufficient certainty to allow responsible actors across the supply chain to continue to operate.

- Respondents highlighted the importance of ensuring policy predictability and consistency to drive the cyber intrusion market. Respondents noted that by establishing rules and laws to address the proliferation and irresponsible use of CCICs, States provide industry actors with clear standards for compliance. The absence of such regulations creates ambiguity that could have negative consequences for the industry.

- In contrast, some respondents highlighted the impact that changing technologies, such as AI, would have on the commercial market, as existing laws may not adequately address the autonomy, speed, and complexity of AI systems. Respondents considered the difficulties surrounding accountability for AI-driven cyber intrusions, where it becomes unclear who is responsible for damages caused. It was noted that the commercial market was likely to become the major driver for AI-driven cyberattacks as a result of financial incentives to do so, and the interconnectedness of the broader technology ecosystem. Respondents further noted the potential impact of emerging AI regulatory frameworks on these risks.

GOVERNMENT PRACTICES

Ensuring 'Responsible Government Activity' Domestically

Emphasising the role of state regulation in addressing risks surrounding the commercial market for CCICs in national frameworks

11 respondents discussed the role that 'national frameworks' should play in outlining States' internal approach to the commercial cyber intrusion capabilities sector, regarding both the development and transfer of CCICs, and their use by law enforcement and intelligence services.

- Respondents recommended that Governments should have in place a strict system of rules, regulations and institutional, independent oversight mechanisms to ensure – where applicable – that CCICs are produced, procured, transferred and used solely for lawful and legitimate purposes.

- Respondents flagged the importance of ensuring that any such framework respected international law, including on human rights and civil liberties.

- Respondents recognised that many States had not released policies addressing CCICs specifically, but noted the important role that existing national cybersecurity strategies could play in responding to the challenge that irresponsible activity can present.

- Respondents highlighted the role of existing laws and procedures in regulating and influencing States' approaches to CCICs, including through:

    - International law and instruments, including international human rights law, international criminal law, as well as instruments to tackle criminality (particularly cybercrime, building on the Budapest Convention), considering both the criminal use of CCICs and the possibility of 'procedural powers such as authorised intercept' for the purpose of criminal investigations and the need to limit use of a CCIC to investigation that it was purchased for.[1]

    - Laws regulating electronic communication and information security, as well as emerging technologies such as AI, including where such measures set general quality requirements for networks and systems to tolerate various disturbances, incidents and attacks.

[1] Council of Europe. (2001). *Budapest Convention on Cybercrime*. https://rm.coe.int/1680081561

- Laws and procedures setting standardised operational requirements based on the relevant legislation serve as regulations and guidelines to ensure a uniform framework for the development, procurement and use of CCICs across law enforcement and intelligence – for example, providing a standardised requirement catalogue translating existing frameworks for use.

- Some respondents suggested that bespoke regulations targeting the proliferation and misuse of CCICs could play a role in reshaping the marketplace and providing a framework for responding to threats, and the need for a single 'point of contact' across Government in cohering such activity. Such laws could build on existing legal and oversight regimes that already govern the use of surveillance technology, providing a new layer of review focused on the trustworthiness and potential risk of these specific technologies.

- Respondents also noted the need for Governments to set an example and be clear about their processes in dealing with vulnerabilities and disclosure. Respondents cited in particular the US Vulnerability Equities Process (VEP) and UK Equities Process as examples in setting out a) a criterion for disclosure, b) a defined evaluation process, c) regular review through an oversight body, with public reporting. Other examples proposed the separation of the defensive and offensive chains in national cybersecurity governance.

Providing clear definitions of what constitutes legitimate Government use of CCICs and establishing procedures to ensure their responsible use

17 respondents discussed the importance of States publicly and consistently articulating where and how the use of surveillance, including via CCICs, is legitimate, in order to set clear 'red lines' on irresponsible activity and misuse.

- Respondents reflected on what 'legitimate use' of CCICs could look like under different State frameworks, highlighting their importance in the interests of national security (such as counter terrorism, managing the threats from hostile States and supporting military operations), and fundamental legal interests, such as in support of the prevention and detection of serious organised crime (such as corruption, or child sexual exploitation and abuse). Some respondents also emphasised that there was a legitimate use of such tools where necessary for advanced penetration testing of particularly sensitive or critical State systems.

- Respondents provided examples of strict frameworks to regulate the Government use of CCICs and minimise associated risks, providing limitations on, and thresholds for, their use. Such frameworks often did not distinguish between commercial and government-developed cyber intrusion capabilities (and would not be expected to) and could impose forms of liability (legal or financial) in event of their abuse.

- Respondents suggested that no single definition of legitimate Government use of CCICs was likely to be appropriate or achievable, stating that a decision around their use should be based on principles such as a) Proportionality – relative to the goal that intrusion would achieve; b) Subsidiarity – ensuring use of CCICs is only allowed when less intrusive options are unavailable; c) Necessity – relative to the role and responsibility of the State; d) Precision – ensuring any use of CCICs is narrowly-targeted and time-limited; e) Checks and balances to hold activity accountable; and f) Security – ensuring that CCIC providers provide an appropriate level of cyber security to their tools.

- Respondents highlighted that the responsible use of CCICs encompasses the need to conform not just with domestic regulations and international law commitments, but also to best practices (on accountability, oversight, precision and transparency), ethics, and non-binding norms (including the norms of responsible state behaviour in cyberspace endorsed by consensus at the UN General Assembly in 2015 through resolution 70/237). These practices should include measures to ensure the use of a CCIC avoids exposing networks to additional cybersecurity risks.

- Some respondents also highlighted the need for governments to provide clear definitions of what constitutes a legitimate use in the context of computer security (including for penetration testing) and research for cybersecurity activities.

- Respondents raised concerns that setting definitions, procedures and controls around what the legitimate use of CCICs should involve could have unintentional impacts on the market. An example was provided of a government limiting its agencies to only allow for the purchase of CCICs for a specific purpose – requiring re-purchase for subsequent uses. This ended up having an unexpected stimulating effect on the market for CCICs, increasing the number of transactions.

- Respondents also raised concerns that where national and international frameworks frame 'legitimate use' as being in the context of national security, through which it could provide loopholes for Governments to avoid accountability. They also emphasised that there can be significant gaps between domestic legal frameworks and their practical implementation, which have led to previous examples of misuse where legal safeguards should have been present.

- Some respondents reflected on the relationship between States' need for CCICs and the provision of 'lawful intercept' functions by communications providers as an alternative mechanism for legitimate surveillance. Respondents highlighted that ensuring compliance with 'legitimate use' could be easier for Governments to apply with alternative lawful intercept capabilities (other than CCICs) but noted the further issues these could raise, including on end-to-end encryption.

Improving cross-Government cooperation and information-sharing regarding decompartmentalising approaches to the market for CCICs

6 respondents discussed issues within existing Government structures around coordinating the use of cyber intrusion capabilities and ensuring consistency in policy approach, and potential mechanisms through which to improve cross-organisational coherence.

- Respondents observed that governments are not homogeneous bodies, and contain an array of entities with conflicting interests. This could make both providing a coherent single government position and taking forward effective action at a state level challenging.

- Respondents considered how governmental bodies could work more closely together to pool knowledge and resources on intrusion capabilities, in order to centralise risk management, education and better understand the potential risks to their citizens that might arise from misuse or overuse. Such joint action could make it easier to operationalise 'responsible' practices for the use of CCICs by bringing together Government users in one place.

- Respondents highlighted how inconsistencies between Government departments and arms-length bodies, particularly across law enforcement, could increase the risk of irresponsible use of CCICs. Organisations with less mature cyber capabilities and lower central oversight were more likely to ignore, misinterpret or misuse powers.

- Some respondents suggested the creation / appointment of a central authority with responsibility to conduct research and development into cyber intrusion technologies on behalf of all national security authorities, in order to minimise associated risks and establish a 'whole-of-government' framework for approaching the market. Such an authority could have responsibility for examining and approving purchasing processes for CCICs, or purchases on a case-by-case basis.

Establishing independent oversight of Government use of CCICs

18 respondents discussed the importance of measures taken to improve oversight around governments' use of CCICs, including mechanisms to facilitate effective audit, and the creation of independent oversight regimes, as well as their effective implementation.

- Respondents proposed that all operations involving CCICs should be recorded in a way that creates a clear audit trail including who used the tool, for what purpose, and the outcome, to ensure they are logged and can be traced for accountability. Such documentation could help to ensure that all operational activities and security measures adhere to a legal framework.

- Respondents highlighted the important role of robust legal and oversight regimes to govern when, how, and why States can monitor or collect information – with the use of CCICs being authorised by a court through the granting of a warrant, or equivalent.

- Respondents considered the necessity of independent review, through a court or alternative competent authority – for example an ombudsman or a parliament – with guarantees of independence, impartiality, and effectiveness. This body could perform both continuous supervision, including *a priori* control, and retrospective accountability on bodies granted permission for the specific use of CCICs.

- However, respondents emphasised the importance of these oversight measures being implemented fully and robustly. They raised concerns about how difficult it could be for independent / judicial oversight to understand the degree to which decisions around the use of CCICs were proportionate: such bodies cannot effectively protect human rights unless fully apprised of an understanding of the technical capabilities of these tools and so States should consider capacity-building or training measures to mitigate this.

- Respondents also noted that in some States' existing systems, the impartiality of courts themselves may be called into question, with the judiciary / oversight mechanisms not fully independent of the executive branch in cases involving alleged Government threats. Some respondents proposed oversight bodies should not just be fully independent from other branches of government, but should also have the power to enforce compliance, conduct investigations, impose sanctions and provide remedies.

Encouraging responsible skills development and management across the CCICs market

11 respondents discussed the role of States in regulating the skills ecosystem that surrounds the market and offensive security community to encourage more responsible behaviour across the development, dissemination, facilitation and use of CCICs.

- Respondents noted the need to ensure responsible practice across the market for CCICs aligns with efforts to grow national talent pools. Governments should prioritise investments in cybersecurity education and training to develop a pipeline of skilled cybersecurity professionals who are equipped to tackle emerging threats and safeguard national interests responsibly. Governments could also help with educating vulnerability researchers to understand the implications of their work and users to help them remain compliant. Some respondents suggested offering grants and funding for research to encourage both current experts and new talent to contribute to the field.

- Respondents highlighted the importance of ensuring efforts to establish best practices for professionals are harmonised internationally (such as through the European Cybersecurity Skills Framework) to ensure that standards are consistent and use the same terminology both in the articulation of competencies and surrounding misuse.[2]

- Respondents considered the possibility of controls to prevent the use of professionals' offensive cyber skills for malicious purposes by a) researchers working with Governments, such as through enhanced vetting requirements, and for b) individuals leaving the Government intelligence community, such as through prohibitions on working for irresponsible organisations – enforced by mandatory reporting and criminal penalties.

- However, respondents flagged concerns around the feasibility of detecting malicious actors within the skills base, due to the rapid pace of growth of talent with cyber intrusion skills and techniques, as well as with the potential infringement such measures could place on the individual rights of researchers.

- Respondents noted concerns around the impact such measures could have on the pool of skilled professionals available to governments. If overbearing, and if workers were not sufficiently compensated, such measures could encourage a 'brain drain' of workers to jurisdictions with looser regulations, and disincentivise individuals with unique skills – like threat researchers – from committing to Government service, further narrowing the band of people the Government can recruit.

- Respondents highlighted the need for open and transparent international debates on this issue, including whether the very idea of skills controls is legitimate or advisable in a context of deep digital divides between and within countries. Respondents proposed that involving all concerned parties in ad hoc fora on skills controls could help avoid creating distrust or excluding important stakeholders.

Measures to improve the transparency surrounding the use of CCICs by States

11 respondents discussed the need for greater transparency surrounding the use of CCICs by States, in order to make it easier for observers to understand where such capabilities are used responsibly, and for legitimate purposes.

- Respondents noted a consistent lack of transparency from States around both the process of how CCICs are acquired, and the purpose for which CCICs are purchased

[2] European Union Agency for Cybersecurity (ENISA). (2022, September 19). *European Cybersecurity Skills Framework (ECSF)*. https://doi.org/10.2824/95989

and deployed by State bodies. This opacity makes it harder to assess the risks and impacts of their use and act accordingly.

- Respondents proposed establishing or enhancing regular reporting processes, whether to a central function providing oversight (such as a parliament) or publicly, detailing how often CCICs are used, the legal basis for their use, and what safeguards are in place.

- Some respondents further proposed requiring real-time public transparency reporting on the use of CCICs to enhance accountability, discourage unlawful surveillance practices, and provide the public with greater insight into the use of CCICs for legitimate purposes.

- However, respondents also noted the difficulties that exist with States reporting on intelligence capabilities, limiting opportunities for public transparency, and suggested that alternative mechanisms for oversight would be more appropriate to avoid publicly exposing sensitive information.

Leveraging Export Controls

Updating export control regimes to more fully cover the sale and transfer of CCICs

27 respondents considered the importance of export controls as a tool through which to control the sale and transfer of CCICs and reflected on the adequacy of existing national and international export control regimes in doing so.

- Respondents provided examples of State implementation of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies as a key tool in balancing controls on CCICs as dual-use technologies.[3] Controls on 'intrusion software tools' and 'IP network surveillance equipment and software' added to the controlled technologies list in 2014 cover some of the CCIC market, and several States have implemented bespoke controls, including on the movement of skills and knowledge.

- Respondents recognised that certain capabilities (including across the exploit marketplace) are not captured under many existing export control frameworks and stated the need to update national and international regimes to reflect technology

[3] World Trade Organisation (WTO). (1995). *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Founding Documents Compiled by the Wassenaar Arrangement Secretariat*. https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf

change. Respondents highlighted concerns around current difficulties in updating the Wassenaar Arrangement and provided diverging opinions on the opportunity and feasibility of exploring alternative arrangements through which to do so.

- Some respondents expressed concerns around the limitations of the Wassenaar Arrangement, as key States relevant to the global market for CCICs are not participants. Respondents called for export control efforts to take into account the need to bridge the international digital divide.

- Respondents also highlighted the risks that updating export control regimes could have in impacting beneficial cybersecurity practices, where tools used in vulnerability research and penetration testing are often dual-use. Respondents proposed that any updates should include carve-outs for vulnerability research and cyber incident response.

Improving the enforcement of export control regimes on the sale and transfer of CCICs

10 respondents discussed limitations in the understanding and enforcement of existing export control regimes by States and industry, and proposed mechanisms to improve compliance and coverage.

- Respondents identified measures within existing export control regimes focused on controlling the end use of CCICs, including End User Certificates (EUCs), limiting the use of exported capabilities to 'combatting terrorism' and to the prevention and investigation of 'serious crimes', in accordance with national law, privacy rights, and subject to obtaining authorisations.

- Respondents noted States' difficulty in enforcing existing export control regimes on cyber intrusion capabilities. CCICs are usually intangible assets, making it difficult for governments to understand and verify the final destination of a product or service transferred outside its jurisdiction, or what its ultimate end use may be.

- Respondents highlighted the need for robust guidance to ensure that all entities operating in the market are aware of their licensing obligations, including the consequences of non-compliance. Respondents also flagged the need for Governments to work directly with private sector companies that develop or sell CCICs, alongside other nongovernmental experts, to reinforce this guidance.

- Respondents proposed enhancing international collaboration and information sharing on export controls to help increase the enforcement of existing measures, addressing the lack of transparency across the market and reducing the ability of firms to evade controls by moving jurisdictions.

Ensuring export control licensing decisions on the sale and transfer of CCICs appropriately take into account human rights considerations

6 respondents discussed whether additional considerations should be made for human rights considerations in controlling the export of CCICs, recognising the particular impact the use of these tools has been reported to have had in infringing on human rights.

- Respondents highlighted examples of where States had placed export controls on unlisted cyber surveillance items, on the basis that their sale may be intended for use in connection with internal repression or the commission of serious violations of human rights and international humanitarian law.

- Respondents recalled the application of a "catch-all clause" in the EU Regulation, which expands the scope of items that are potentially subject to export control beyond those already covered by the Wassenaar Arrangement, enabling EU Member States to refuse an export licence for them if there is a clear risk that the technology to be exported might support serious violation of human rights.

- Respondents advocated for the use of controls to prevent CCICs from being sold to customers with poor human rights records, and for their enforcement through international cooperation, ensuring that vendors could not bypass regulations by operating in jurisdictions with weaker laws. Respondents highlighted the Export Control and Human Rights Initiative as one such example of international cooperation but noted that the uptake of equivalent approaches by States remains inconsistent between regions.[4]

Improving transparency surrounding export controls over the sale and transfer of CCICs

5 respondents considered the potential role of improved transparency and public oversight over the use of export controls restrictions on the sale and transfer of CCICs, to aid with accountability and audit.

- Respondents advocated for enhanced record-keeping on the distribution and export of CCICs to ensure operations can be reviewed, evaluated, and audited. This included proposals for recording employees involved in product development.

[4] US Department of State. (2023, March 30). *Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy*. https://www.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy/

- Some respondents proposed that States should build mandatory and regular audits into licensing practices along with punishments for non-compliance, establishing independent supervisory bodies with appropriate powers and resources to carry out this task.

- Some respondents also argued that such licences, or the outcomes of such audit processes, should be made public, in order to supplement know-your-vendor data and enable the broader research community and civil society to serve as crucial external accountability mechanisms.

- However, respondents noted the technical limitations of such audits, creating a significant bureaucratic workload for governments above existing practices, and may be unachievable for States under significant resource constraint. Some respondents argued this would also further burden private sector actors, impacting the cybersecurity industry's ability to respond to rapidly evolving threats (although others argued that this would be an acceptable burden).

- Respondents also noted the risks that the publication of export licences could create, exposing commercially-sensitive or personally-identifiable information which could violate privacy rights, and impact companies' ability to recruit researchers. Respondents also highlighted that publishing national audits would intrude sensitive matters for national security – out of line with States export controls practices in other areas.

Leveraging Procurement Power

Establishing procurement practices to control Government engagement with the market for CCICs

14 respondents discussed how State procurement controls could be used to prevent Government organisations from engaging with or inadvertently supporting irresponsible commercial actors across the market for CCICs, and to send a clear message to industry around unacceptable activity.

- Respondents highlighted how, where Governments choose to purchase cyber intrusion capabilities from private companies, they inadvertently create and maintain an industry that might not exist without well-funded Government contracts.

- Respondents proposed that, given their influence in incentivising this marketplace, Governments should hold each other accountable to ensure their policies uphold international law and security, human rights, and protect the stability of cyberspace.

- Respondents suggested that procurement requirements could be enforced both through regulatory controls – giving Governments legal powers with which to bar CCIC vendors from procurement by the State, and internal processes acting as guardrails across Government practices, including specific definitions as to which authorities are authorised to manufacture, import, purchase, hold, display, offer, sell, rent and use CCICs.

- However, respondents expressed concern around the potential burden of implementing and regulating procurement controls across wide-ranging and complex bureaucracies – an obstacle to tackling this fast-moving and -adapting challenge.

- Respondents also expressed concerns that a lack of transparency around the market for CCICs could make such processes difficult to implement with nuance. Blanket bans or overly restrictive controls on CCICs could have adverse impacts, pushing the industry underground, towards irresponsible State and non-State actors, and limit legitimate cybersecurity research and development.

Leveraging Government procurement power to encourage responsible behaviour across the market for CCICs

7 respondents considered how, as States represent the main customers for the CCIC market, leveraging procurement power to encourage or mandate responsible activity by providers can play an important role in discouraging irresponsible activity by commercial actors.

- Respondents proposed that a process for screening and certifying vendors could verify their compliance with both national and international cybersecurity and human rights standards, ensuring that only trusted suppliers provide these sensitive capabilities, to the benefit of purchasing State customers.

- Some respondents cited the US Executive Order on the Government use of commercial spyware posing risks to national security as a model for government procurement controls.

- Respondents suggested such screening could build on establishing and enhancing 'Know Your Vendor' and 'Know Your Customer' requirements to create a more consistent reporting environment across the market. This would allow Governments to check where their prospective supply chain might include firms on restricted lists before awarding contracts, as well as mitigating national security risks by potentially disclosing vendors' corporate structure, affiliations, and foreign ownership.

- Respondents highlighted how controls could be used to incentivise more desirable behaviour across the industry, with preferential treatment for companies that are providing services in a responsible way, alongside producing and sharing anonymised case studies of good practice with the market.

- However, respondents also expressed concern around the feasibility of putting such requirements into practice, highlighting a lack of precedent for requiring such extensive disclosure of investor and supply chain information and the obstacles posed by the sensitivity of the market. Some respondents highlighted that such processes could overburden suppliers and provide preferential treatment to larger established vendors, reducing market dynamism.

- Respondents suggested that such measures would be more difficult for smaller States to implement, given limited capacity. Respondents proposed to improve information-sharing of templates or guidelines around vendor certification.

Targeting Irresponsible Actors

Identifying countermeasures through which to target irresponsible actors across the global market for CCICs

11 respondents discussed the role of potential punitive State action against irresponsible actors across the CCIC industry. Respondents highlighted that, alongside restricting exports and controlling procurement, stronger policy levers could be used to send a strong signal to the market.

- Respondents encouraged States to make better use of sanctions as part of a toolkit of countermeasures against irresponsible actors across the market to impose a cost on those involved in carrying out, facilitating, or benefiting from the misuse of CCICs. These could include financial sanctions, visa restrictions, or limitations on accessing intellectual property held within the sanctioning State.

- Respondents provided examples of the use of sanctions or equivalent policy tools to target irresponsible CCIC actors, and their impact – reflecting how targeted companies might attempt to rebrand, move jurisdictions, or otherwise reform and continue operating. As such, accountability measures that targeted both the commercial entity and their broader ownership structures and supply chains would be most effective.

- Respondents highlighted how the corporate structures and supply chains for CCICs are often complex and with a wide geographic distribution. International cooperation would be essential to overcoming these challenges to regulatory and legal action and for maximising the impact of sanctions or equivalent levers.

International Cooperation

Closer international collaboration and coordination between States on approaches to the market for CCICs

25 respondents reflected on the international nature of the problem, with many highlighting the need to ensure that any approach to the market for CCICs focused on addressing shared threats also reflected diverse State positions on the issue.

- Respondents emphasised the importance of information-sharing to improve State awareness of the risks surrounding irresponsible activity across the market for CCICs, as well as understanding of possible mitigation mechanisms.

- Respondents identified a number of existing international and multistakeholder fora already providing constructive dialogue and challenge on the issue. These include the ongoing discussions in the UN Open-Ended Working Group on security of and in the use of information and communications technologies; the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware; the European Parliament's PEGA Committee to investigate the use of Pegasus and equivalent surveillance spyware; and the Paris Peace Forum multistakeholder working group on cyber mercenaries.

- Respondents also highlighted a number of existing regulatory frameworks that could be used more in the future to cohere joint consideration of the issue and called for further engagement / action to be taken through these fora. These include the Budapest Convention, the Malabo Convention, the Organisation for Economic Cooperation and Development, as well as through regional organisations. Respondents highlighted the implementation of the EU Dual-Use Regulation and EU cybersecurity frameworks such as the Cyber Resilience Act (CRA) and the NIS 2 Directive as examples.

- Respondents emphasised the need to ensure participation of stakeholders from the Global South, as well as converging discussions with ongoing open processes under the United Nations. It is important to ensure that all States engaging with and affected by the market are given the opportunity to be active contributors in shaping global approaches. Some respondents suggested fostering regional public-private collaboration, including through the creation of regional partnerships to facilitate information sharing, joint training, and resource-sharing initiatives.

- However, some respondents also raised concerns that accommodating more stakeholders would come with the risk of lowering standards and hindering joint action. Stakeholders proposed that ensuring the principles and practices

established are robust and effective should be an initial priority, even if this would only be achievable with a smaller group of countries signing on initially.

Reducing inconsistencies between existing processes and regulations relating to CCICs

11 respondents highlighted the need for a more aligned approach between States, harmonising the use of existing definitions, legal architecture and best practices to give companies consistency and address enforcement gaps.

- Respondents raised concerns around how a lack of uniformity in approach was making it harder for companies to operate responsibly in the commercial market for CCICs, with no clear articulation of what best practice and irresponsible activity looked like, and for States to respond to cross-border activity. Respondents also flagged the risk that such inconsistencies could make the enforcement of policy levers more difficult – hindering investigation into irresponsible action and making it easier for commercial actors to move to more favourable jurisdictions.

- Respondents identified the need for uniform standards, procedures and registries surrounding CCICs, particularly with regards to information held by governments on companies, and risk thresholds. Respondents highlighted how searches carried out in export licensing and procurement decisions could be helped by data, and a better understanding around how decisions are made across law enforcement and intelligence communities, highlighting the European Cybersecurity Skills Framework as a potential model to use.

- Respondents flagged inconsistencies in legal frameworks as a blocker to joint action against irresponsible actors, such as in prosecuting cross-border cases. A lack of consensus makes it harder for authorities to act, requiring States to act individually or in small groups to identify and counteract undesirable practices. Respondents provided the example of States making commitments through the Budapest Convention to improve the use of mutual legal assistance, shared procedures and access to evidence as one such example of addressing this issue.

- Respondents emphasised the importance of involving all stakeholders in these discussions, proposing that a regular dialogue between vendors, governments, and other actors could help to shed light on vendor drivers and incentives to arrive at policy and governance solutions that align with industry realities.

- However, some respondents cautioned that the sensitivities around States' use of CCICs may make extensive information-sharing or harmonisation of approaches between States difficult. Some respondents also raised concerns around the potential impact of an international regime on the market, causing CCIC vendors to

raise prices, expand to non-participating customers and consolidate, reducing opportunities for innovation.

Aligning cyber capacity-building initiatives with efforts to address the proliferation and irresponsible use of CCICs

3 respondents highlighted the need to avoid creating a 'tiered system' for States in which a large number of countries are excluded from accessing CCICs in spite of their legitimate uses. Respondents cited cyber capacity-building as a way of supporting States to achieve 'best practices' with regards to a responsible approach to the market.

- Respondents proposed that States with access to advanced cyber capabilities should engage in inter-regional capacity-building efforts to share knowledge and resources and help less-developed nations build their own defensive cyber capabilities through infrastructure support, policy guidance, and intelligence sharing – alongside the regulatory mechanisms to needed to support them.

Developing an international oversight mechanism for the global market for CCICs

9 respondents considered the need for new mechanisms through which to help implement international coordination, such as setting standards, carrying out audits, and providing accountability.

- Some respondents suggested that in order to implement and enforce a joint approach, the Pall Mall Process should encourage the creation of a new international governance body to standardise the regulation of CCICs and encourage compliance / accountability. Respondents proposed that CERTs, or Data Protection Authorities across the EU, could provide a good model for joint action.

- Respondents considered the potential role of such an authority in aligning the use of policy levers such as export controls and procurement requirements, and potentially investigating claims of misuse – facilitating litigation, measuring harm of attacks, assisting victims to access redress and potentially investigating claims of misuse.

- Respondents further proposed the need for an international certification scheme for CCICs, building on the model of the Montreux Document on Private Military and Security Companies and accompanying International Code of Conduct Association

(ICoCA), with a 'code of conduct' for States and businesses, alongside a complementary industry body.[5]

- Some respondents highlighted that such a certification scheme could also be used to drive improved transparency across the market, publishing information on the market, and rating States and private firms based on their adherence to international norms around CCIC.

- However, as with domestically-implemented oversight, respondents raised concerns around the bureaucratic burden and transparency challenge of setting up any international mechanism, alongside the ability of such a body to keep pace with technology change.

- Some respondents shared concerns that such bodies would be inadequate in practice, due to State sensitivities around the particular national security context of the procurement and use of CCICs, complicating information-sharing across jurisdictions.

Updating or better implementing existing international frameworks

12 respondents discussed the role of international frameworks, including laws and norms, in directing States' relationship with the commercial cyber intrusion marketplace, and constraining irresponsible activity.

- Respondents emphasised the importance of consistently applying and enforcing existing international law and frameworks. Moreover, respondents highlighted the role that international laws and norms can serve to solidify common understandings and commitments among States, setting global standards for engagement with the market for CCICs, and a basis to restrict access and establish penalties following irresponsible behaviour.

- Respondents reflected on how existing normative frameworks could / should be applied in the context of the market for CCICs, including the norms *on the security of and in the use of information and communications technologies* adopted in the UN General Assembly's First Committee in 2015 in the context of the Group of Governmental Experts (GGE), and highlighted language relating to CCICs published

[5] International Committee of the Red Cross (ICRC), & Federal Department of Foreign Affairs of Switzerland. (2008). *The Montreux Document: On pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict*. https://www.icrc.org/sites/default/files/event/file_list/montreux_document_en.pdf

in the Threat section of the 2024 Annual Progress Report of the Open Ended Working Group (OEWG).

- Respondents highlighted in particular Norm i: “States should take reasonable steps to ensure the integrity of the supply chain so that end-users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.”

- Some respondents further proposed the establishment of new norms, including for the development of commitments that States should contract with providers of CCICs only where it satisfies particular conditions and respects international law, including international humanitarian law and international human rights law.

INDUSTRY PRACTICES

Encouraging Responsible Behaviour

Publishing principles and processes the company operates under to ensure responsible use

7 respondents discussed the impact of companies setting out clearly and publicly the ethical standards they abide by, and the processes they use to put them into practice.

- Respondents highlighted policies and processes published on the websites of CCIC vendors, including on human rights standards.

- Some respondents further described how regularly-published reports could be used to outline how these were put into practice and proposed appointing an external ethics committee to monitor whether a company was upholding the policies and processes as promised.

- Respondents emphasised the importance of this approach for transparency and accountability, to manage the expectations of potential customers on how use conditions would be enforced using end-user licence agreements.

- However, respondents noted that many companies in the CCIC market operated opaquely, without public-facing websites, let alone published policies.

- Respondents also noted that whilst many companies have made ethical pronouncements, these were often in response to public allegations of irresponsible behaviour. There were concerns that such approaches might 'ethics wash' a company's image, particularly where not given full sight of a company's operations because of confidentiality concerns, and give any such monitoring a lack of credibility.

Creating voluntary principles or a code of conduct for the CCIC industry to adhere to

9 respondents discussed how companies could sign up to a code or standards defining responsible behaviour, providing a market signal to encourage wider behaviour change.

- Respondents proposed the creation of a code of conduct focused on protection of human rights, drafted with the involvement of civil society organisations. This would include clear guidelines to the scenarios in which CCICs could be deployed legitimately and what level and kind of oversight of their use was required.

- Respondents highlighted the industry principles released by the Cybersecurity Tech Accord in 2023 as a useful example of good practices (although designed for companies whose platforms may be targeted with the use of CCICs, not for companies working in the industry themselves).[6]

- Respondents cautioned that any code of practice would need to reach a critical mass of support, to avoid signatories impacting their own market position. This would mean such principles would need to be flexible, given the significant differences of size, capacity, and resources between different organisations involved.

- Respondents noted that such a code could help to reduce the burden on companies to identify and implement responsible behaviour and would allow for anonymised case studies of specific examples of good practice.

- Some respondents further proposed that such a mechanism should be accompanied by independent oversight, to ensure companies abided by set principles.

- However, some respondents also remained sceptical about the potential of such measures to change market incentives – existing reputational damage to the industry had made little change to overall business practices, and only impacting profits could affect market change. Some respondents also highlighted the difficulties with any mechanism providing credible oversight where confidentiality could be a concern, and without a means of enforcing accountability.

- Some respondents proposed a number of methods for incentivising adherence to principles or a code of practice, including support from governments in the form of tax breaks or grants, preferential procurement or expedited export licencing. Further proposals suggested such principles could form the basis for a form of international certification.

Having clear whistleblowing procedures in the case of irresponsible activity

5 respondents discussed whistleblowing procedures as a mechanism for encouraging reporting of suspected irresponsible use.

- Respondents described corporate whistleblowing policies and provisions for anonymous reporting by employees or other stakeholders. For some companies,

[6] Cybersecurity Tech Accord. (2023). *Cybersecurity Tech Accord principles limiting offensive operations in cyberspace*. https://cybertechaccord.org/uploads/prod/2023/03/Cyber-mercenary-principles_Tech-Accord_032723_FINAL.pdf

whistleblowing reports could also be submitted via third parties, rather than directly to the company.

- However, respondents also emphasised the need for clear and independent channels for discreetly reporting misuse of CCICs, rather than to the company itself. Respondents gave the example of an email address provided by the US State Department for reporting on the misuse of spyware, but likewise highlighted the need for robust independent mechanisms to protect governmental whistleblowers.

Managing Vulnerabilities and Exploits

Promoting widespread, standardised, and transparent vulnerability disclosure programmes and policies

7 respondents discussed the role vulnerability disclosure programmes and policies played in offsetting the attraction of selling vulnerabilities on the market that might then be exploited in CCICs, and in enhancing wider cybersecurity to mitigate the impact of irresponsible activity.

- Respondents described an "arms race" between two sets of vulnerability researchers – with one group informing the software or platform owner so they could fix the issue, and the other selling the vulnerability on the marketplace or via a broker, where it might end up being used in a CCIC. Respondents noted the complex and changing role of 'exploit brokers' in facilitating the sale of vulnerabilities and exploit chains throughout the market.

- Respondents saw clear and transparent vulnerability disclosure programmes and policies – setting out both how someone should approach a company when they discover a vulnerability and how the company will act in response – as essential for strengthening the approach of researchers looking to patch problems.

- Respondents emphasised that the overall principle behind having a vulnerability disclosure policy was to enable all providers to understand and address risks. Proposed practices included:

    - Policies to inform decisions around where and when disclosures to a third party / public could be appropriate (such as in response to a major incident or when providers fail to address risks in a timely manner), as well as when disclosures could be harmful.

    - Transparency measures, including around when and how vulnerabilities have been detected, to help understanding of attacker behaviour.

  - Oversight measures such as through governance committees considering disclosure decisions on a case-by-case basis in line with that policy.

- Respondents highlighted that software / platform providers should adhere to international standards that set out how vulnerabilities should be handled and / or disclosed – ISO/IEC 29147 and 30111 – to encourage consistency and build trust.

- Some respondents called for more explicit legalisation around legitimate / responsible vulnerability discovery by governments. Clear definitions of responsible behaviour for researchers could provide an incentive to engage with vulnerability disclosure processes rather than the commercial market. Respondents pointed to the definition of "good faith security research" contained in US law as a useful example.

Supporting and expanding bug bounty programmes

9 respondents discussed bug bounty programmes as an important subcategory of vulnerability disclosure programmes, offering researchers a reward when they discover a vulnerability as an alternative to the commercial marketplace.

- Respondents cited bug bounty programmes as important for reducing the financial incentives that drive both the products (vulnerabilities) and the talent discovering them (hackers) to the commercial marketplace by providing an alternative that still rewards hackers for their work.

- Respondents emphasised that while a number of big tech companies already had effective programmes – Google and Meta were named by respondents as specific examples – these needed to be expanded across the industry to make them more widespread and harmonised to make it easier for researchers to engage.

- Respondents emphasised the important role bug bounty programmes play in strengthening overall cybersecurity, by ensuring vulnerabilities were reported directly to those who could fix them – and in doing so would remove the entry points required by CCICs to function.

- However, some respondents pointed out that as private buyers offer higher prices than bug bounty programmes, bug bounties did not provide sufficient incentives to encourage a change in behaviour if researchers were financially motivated. Respondents proposed that bug bounty programmes should pay out higher rewards to compete with the commercial market (although other respondents questioned the impact that doing so could have on vulnerability prices).

- Some respondents expressed concerns that some vendors used bug bounty programmes as a way of silencing researchers and avoiding external pressure to patch a vulnerability, through discouraging public disclosure.

Ensuring strict security protocols govern internal research and use

4 respondents detailed the importance of security procedures for internally-developed vulnerabilities and exploits in order to guard against their misuse or contribution to irresponsible activity.

- Respondents highlighted the importance of placing a strict compartmentalised structure in place in their in-house research teams for vulnerabilities and exploits. This included limiting researchers' access to other teams, and vetting individuals provided with oversight of entire vulnerability chains and how they fit together to limit the risk of unauthorised use or disclosure.

- Respondents provided examples of employing vulnerability researchers under strict non-disclosure agreements, prohibiting them from selling or engaging with vulnerabilities outside of their work for the company.

- Respondents also considered the security procedures needed for access to the exploits developed in-house, including through an assessment and approval process for access, encryption, password control, and access expiry after a certain period of time. This was accompanied by rigorous monitoring of the use of the exploit, and fingerprinting on when exploit was used, and who by.

- However, some respondents raised concerns around the technical feasibility of such access procedures, pointing to successful and unsuccessful analogues for supplier / user requirements in other industries, including in finance, and across critical national infrastructure.

Managing Suppliers

Ensuring robust vetting of suppliers

9 respondents described the importance of ensuring suppliers were reliable and operating responsibly in order to help promote responsible activity further up the supply chain within the cyber intrusion marketplace and avoid being caught out by irresponsible actors.

- Respondents emphasised the significant security risk that exists in working with third party suppliers within the cyber intrusion market, particular with vulnerability researchers and brokers. Some respondents proposed that all involvement of third-

party suppliers in this market represented too high of a risk, and that products should be built from elements researched and developed in-house.

- Some respondents proposed security measures needed to limit external suppliers' access to or contact with the company's wider systems, including segregating the servers that external suppliers connect to for support and performing regular security audits with this risk in mind.

- Respondents reflected on the vetting process required to work with independent researchers offering to sell exploits or vulnerabilities – based around verifying their identity, assessing their track record, determining their standing in the wider community, and their motivation for selling a particular item. Some respondents suggested additional checks including a) vouch-safes on new researchers from existing employees; b) third party audits of potential researchers; and c) keeping the vetting of all third-party researchers under regular review.

- Respondents highlighted the importance of 'trust' in working with third party suppliers for cyber intrusion capabilities and relying on existing researchers to 'vouch' for new contacts and potential collaborators.

- Some respondents suggested that a trust-based approach to suppliers could be more widely applied and institutionalised, similar to the way in which different entities within the US national security community grant mutual recognitions for security clearances.

- Respondents emphasised that an approach to trust and vetting should not only be applied to researchers, but also their contributions – describing measures to test the supplier's contribution before incorporating it into a wider product – and in some cases holding them accountable for their contributions (such as through introducing a code signing requirement).

Creating greater supply chain transparency

8 respondents discussed how increasing the visibility and transparency of product supply chains could provide both customers and researchers / vendors with reassurance around their own impact on the CCICs market.

- Some respondents highlighted the principle of 'transparency by design' and, while acknowledging this might be considered radical in a traditionally opaque market, how it could be applied to all elements of the CCIC supply chain, both at a market level and within individual vendor organisations. Respondents referenced the concept of a Software Bill of Materials (SBOM) as an example to inform the development of transparency requirements in practice. Existing models for SBOMs

have not been applied to CCICs, but could play a role in enhancing the cybersecurity of digital products, through detailing all the parts and dependencies for a software package and is designed to give vendors and developers greater insight into its components with a view to better tracking the cybersecurity risks.[7] A 2021 US Executive Order made SBOMs mandatory for software used in US federal IT systems. The EU's Cyber Resilience Act also requires SBOMs from manufacturers of categories of products with digital elements, alongside 'security by design' requirements to potentially reduce the attack surface for CCICs.

- Respondents considered how the changing software liability landscape could impact companies operating in this space, with liability decisions on the misuse of software providing a potential avenue for victims to seek out recourse, helping to deter vendors and / or operators from irresponsible activity.

- Respondents suggested that this approach to transparency could be applied to open-source components as well, ensuring the provenance of all open-source code was verified, in order to guard against potential attacks on the open-source supply chain.

- Some respondents suggested how such a transparency approach could be integrated in procurement practices within individual vendors, tailored to customer needs. Respondents described how exploits should be purchased under exclusivity only, allowing the company to control its use and vouch for this. Customers could be given clear guides to the origin and details of product components.

- However, other respondents also highlighted concerns about the feasibility of this approach – given the market's opacity was such that it was almost impossible to truly verify the source of any particular development.

- Respondents also raised concerns that this approach would improve transparency to end use customers, but not ensure full transparency across the wider market. Respondents noted such measures could create safeguarding risks for the individuals involved.

[7] United States Cybersecurity Infrastructure and Security Agency (CISA). (2024). *Software Bill of Materials (SBOM)*. Cyber Threats and Advisories. https://www.cisa.gov/sbom

Managing Customers

Ensuring robust client and customer vetting practices

18 respondents noted the importance of commercial cyber intrusion companies having procedures in place to ensure they were only selling products to customers that would deploy them in a responsible manner – but detailed a number of different approaches to this.

- Respondents noted that many vendors limited sales of cyber intrusion capabilities to Government end-users and emphasised that they should adopt 'know your customer' protocols and processes to make sure that customers were who they claimed to be.

- Some respondents noted the need for vendors to limit sales to a 'good list' of 'trusted partners' that they believed had a track record of meeting the highest standard of responsible behaviour and had robust guardrails and oversight processes in place. Other respondents proposed opting for a reverse approach, holding a 'bad list' of customers they would not sell to, because of a risk of irresponsible use.

- Respondents described due diligence procedures for potential customers to obtain proof they were acting in an official capacity, before then insisting on non-disclosure agreements before sharing their capabilities portfolio.

- Respondents also pointed out that the opacity in this market made it difficult for vetting processes to work effectively in practice, with the widespread use of shell companies making it difficult for sales agents to determine the location of the ultimate end-user.

- Respondents detailed potential vetting procedures for potential Government customers, making use of initiatives like the UN Guiding Principles on Business and Human Rights, which details principles businesses should adhere to in areas such as human rights or anti-corruption, to inform their approach to considering customers. These processes can include assessing against ratings and guidance produced by the vendor itself; by host governments (e.g. human rights assessments or informal guidance); by international organisations such as UN agencies or the European Union; or readily-available open source material such as the Reporters Without Borders World Press Freedom Index, the Economist Intelligence Unit's Democracy Index, or Freedom House's Freedom in the World ratings.

- Respondents noted the importance of considering this vetting and risk assessment process for both country of destination and the end-user customer – in some States, for example, a particular Government agency or law enforcement arm may have their own risks as users that do not apply to the country as a whole. Respondents also suggested that this vetting should be an ongoing process, and even once a customer

had been approved and sold to the same procedures were followed as part of ongoing monitoring assessing the risk of a particular customer. Additional monitoring, shorter software licences, or similar measures could be considered on a case-by-case basis.

- Respondents suggested keeping this vetting process relatively independent from the sales operations by having it carried out by e.g. legal teams, multistakeholder committees, or independent third parties.

- However, respondents flagged some difficulties with this vetting approach towards individual Government customers. They noted the high degree of ambiguity in determining what sources to rely on to determine whether a Government customer was 'responsible' or not. Respondents raised concerns that Government statements could not always be relied upon, and there were potential political and reputational ramifications for refusing sale to particular governments. Respondents also expressed concerns around the financial impact of such decisions, noting that a lack of internationally-agreed shared vetting criteria and processes left companies open to competition from new companies based in jurisdictions less concerned about this.

Having mechanisms in place to restrict use

13 respondents mentioned measures companies have or could put in place to restrict the use of their products, through both legal and technical means. Where customer governments did not have fully robust legal oversight mechanisms constraining their use, vendors could seek to bind customers' activities in an equivalent way.

- Respondents highlighted software licensing as an important element of guarding against misuse – legal contracts binding the end-user to certain conditions, including a prohibition on sub-licensing or transferring the products to other users, which could be revoked if breached. Respondents described how licences could restrict the number of targets for intrusion products, be time-limited or have periodic 'sign off' points. Whilst not always technically enforceable, respondents stressed the potential diplomatic, operational, and financial impacts of being perceived to be in breach of contract.

- Respondents described software licences as unworkable under particular business models, such as where products were sold on the basis of exclusivity (particularly true in the case of vulnerabilities), or limited use.

- Respondents described further technical measures that could be put in place to control the use of products, particularly through links to specific hardware. These included:

- Requirements that the system be installed by the company itself on designated machines, with password controls, and / or the use of the tool requiring the direct input of people trained directly by the company.

- Ensuring intrusion products were a 'black box' that clients could only use as a complete product, without sight of any underlying code or components; with end code obfuscated and encrypted to guard against its unauthorised use or transfer.

- The installation of remote 'kill switches' to allow vendors or customers to restrict use in extreme cases of misuse or malfunction, or shut down product use completely.

- However, some respondents were sceptical about the efficacy of these measures in practice and questioned whether companies would ever limit a customer's access to a product unless they themselves were facing legal action. Respondents also noted that this was a measure that only applied to the provision of an end-to-end product such as spyware – once a vulnerability or exploit code has been sold it cannot be revoked.

Having clear procedures for monitoring, auditing and investigating customer use

11 respondents discussed how companies could / should monitor how its customers were using its product, and how this could be used to audit or investigate potential irresponsible use.

- Respondents noted that vendors earlier in the supply chain selling to commercial customers rather than directly to Governments needed to ensure that they had the contractual right to audit sales records to determine that their products had not been sold to unapproved end-users.

- Respondents emphasised the importance of requiring customers to maintain comprehensive logs of their use of a product, and embedding this tracking into the architecture of the tool so as to ensure any misuse could be quickly investigated and attributed.

- Respondents highlighted the necessity of carrying out regular audits of customer use of their tools to ensure compliance with the terms of their contracts. Such activity could be carried out by technical teams or built-in mechanisms trained to spot system anomalies that might suggest suspicious use or attempts to circumvent particular restrictions, or else carried out on-site, with greater access to contracted systems because of strict licensing rules. Other respondents proposed the need for regular independent auditing by third parties to provide an additional layer of accountability and help spot potential misuse early.

- Some industry respondents detailed their procedures around investigating suspected misuse and the consequences that a customer might face, including through review of a customer's technical and generic audit logs with operational data removed, legal procedures (in an independent jurisdiction to maintain independence), and follow-on measures. This could include further training, enhanced monitoring or more frequent auditing spot-checks, and technological restrictions on the product's use.

- However, many respondents remained sceptical about the extent to which comprehensive auditing was truly possible – as customers would not want to buy a product that they might perceive was 'spying' on them, particularly given the highly sensitive uses of these capabilities. Respondents emphasised vendors' limited ability to both investigate allegations fully or to force customers, as sovereign States, to institute robust grievance procedures or investigate product misuse.

Providing customer training and / or guidance that reinforces responsible use

6 respondents discussed the need for companies to provide guidance and / or training to end-users to encourage responsible use.

- Respondents highlighted that vendors provide their customers with clear guidance about how their products should be used responsibly. This could include instructions reminding end-users of their obligations under international law, particular technical steps to take to guard against the unintentional proliferation of the capabilities, and guidance about what to do if they believe wrongful use has taken place.

- Some respondents recommended vendors provide extensive training to customers on the ethical and legal responsibilities around use of their technology. This could include subjects such as human rights impacts and the principles around lawful intercept, and could involve real-world scenarios with ethical dilemmas.

Retaining customer information, potentially with a view to disclosure

5 respondents mentioned the need for companies to maintain a comprehensive log of their customers and their activities for accountability purposes.

- Respondents agreed on the importance of, for accountability purposes, retaining customer data for a sufficient period of time to allow for the traceability of their products and services by the company or relevant authorities.

- Some respondents stated that vendors should be required to disclose information about their customers, the capabilities sold to them, and the intended uses through

mandatory reporting to encourage accountability. Further proposals included publishing through a ‘global transparency portal’ details about the legal frameworks governing the tool’s use to discourage sales to irresponsible users.

OTHER PRACTICES

Supporting Victims of Misuse

Increasing awareness of the risks posed by CCICs and enhanced support for victims

8 respondents highlighted the problems surrounding awareness of the threat posed by CCICs to individuals at the highest risk of their misuse, including among civil society advocates, journalists, politicians, dissidents, and those in high profile commercial roles.

- Respondents highlighted the need to carry out awareness-raising and cybersecurity training to help mitigate some future risk. Respondents likewise proposed to raise awareness of the support and resources available from Governments and third-party organisations, including for raising complaints, legal or technical assistance, incident response, and system recovery.

- Respondents emphasised that not enough support from governments existed for individuals targeted, or at risk of being targeted, by CCICs. They noted that as victims may not be able or willing to turn to their governments, third party providers currently take on the responsibility for providing this support.

- Respondents expressed frustration around the lack of support available from States for individual victims and called for commitments around the provision of further assistance, including compensation and programs offering technical, legal, and mental health support. Some respondents proposed that this could be enhanced through the establishment of a global reporting system, where cases of suspected misuse of CCICs could be reported and tracked, and an international case clearing house to provide support in investigation and remediation.

- However, some respondents highlighted that such a clearing house could duplicate or run counter to existing law enforcement efforts, and that legal concerns over confidentiality and protection of personal information would hinder its effective functioning.

Removing impediments to investigations into, and prosecutions for, the misuse of CCICs

14 respondents discussed the impediments that exist to victims of the abuse of CCICs and other relevant parties seeking legal recourse because of legal ambiguities and bureaucratic processes. These barriers make it harder for victims to recover and hinder legal action being taken against irresponsible actors.

- Respondents highlighted ambiguity and inconsistency surrounding the national and international instruments which aim to regulate CCICs as a major blocker to individuals seeking legal recourse after being targeted with these tools. Some respondents proposed that governments should subject companies involved across the market for CCICs to a comprehensive legal framework grounded in international human rights law to ensure victims can get meaningful access to justice and remedy. Some respondents proposed to mitigate this by creating an independent global assistance mechanism that could handle complaints, investigate misuse, and provide support to victims.

- Respondents also highlighted the need to shorten response times and enable quick access to law enforcement for victims. Systems for accessing justice for spyware abuse can be highly inefficient, often leading to re-victimisation and undermining the right to an effective remedy. Victims face numerous legal and procedural obstacles, including lack of transparency and notice, challenges to their legal standing to bring claims, limited cross-border cooperation, and inadequate support mechanisms, which can prevent them from obtaining effective remedies.

Encouraging a 'counter CCIC' industry

4 respondents discussed the need to establish and grow a commercial industry focused on countering the irresponsible use and misuse of CCICs.

- Some respondents highlighted that the number of victims of the misuse of CCICs was significant, and growing, beyond what could be supported by a handful of organisations or dissuaded through economic measures.

- Respondents proposed to mobilise the private sector in responding to the threat presented by the irresponsible use of CCICs, through providing incentives to make this new market economically lucrative, in order to develop scalable solutions to effectively detect, study, and block CCIC attacks.

Supporting Threat Researchers

Increasing the visibility and publishing of research into the threats presented by the irresponsible use of CCICs

12 respondents highlighted the significant role that threat researchers from across academia, the non-profit sector, and technology industry have played in uncovering and understanding the threats presented by the irresponsible use of CCICs. They emphasised the need to encourage and build on this research moving forward, both to better understand specific threats, and the trajectory of the market in response to changing technologies and Government action.

- Respondents emphasised that reporting since 2019 on the scale and impact of the misuse of CCICs has played a key role in raising awareness on the issue and encouraging governments to take national and international action.

- Respondents highlighted the important role that detailed technical reporting into detected intrusions has played, both across significant networks / systems and on the devices of individual victims. These efforts have allowed for external threat researchers to discover new CCICs and help build defences against existing capabilities.

- Respondents also noted the role that open-source supply chain analyses can play in helping to understand business structures and relationships that underpin commercial actors across the market for CCICs, as well as in informing Government responses to irresponsible activity.

- Respondents reinforced the need to reinforce and grow these efforts where appropriate, noting how inconsistent cooperation between threat researchers could hinder the impact and reach of some work, at times risking duplication. Additionally, some respondents expressed interest in receiving greater feedback from governments on the threat research they have shared.

- Respondents noted that governments should have more of a role to play in investigating and documenting the misuse of CCICs.

- Threat research and technical attribution was also noted as a means to reinforce informal industry transparency mechanisms, enabling the tracking of tool use and encouraging proactive disclosure by vendors of misuse.

Providing legal protections for threat researchers

12 respondents highlighted concerns around the pressures researchers face because of legal cases brought against them as a result of their work, both from large commercial entities looking to remove negative information from being made public, and from governments.

- Respondents discussed the use of strategic lawsuits against public participation (SLAPPs) by CCIC vendors to force the takedown of information about their corporate and business practices available online, which can be particularly effective where research organisations are not resourced to support complex legal cases. Under the EU Anti-SLAPP Directive, adopted in May 2024, EU Member States are obliged to provide protection from this kind of activity in national law, including by enabling courts to dismiss manifestly unfounded proceedings via an accelerated procedure

in order to minimise their impact on the victims and provisions for the recovery of costs of the proceedings by defendants and potential penalties.[8]

- Respondents further considered cases in which governments have used national security as a pretext to legal threats to prevent the disclosure of spyware usage or misuse.

- Some respondents proposed commitments towards legal protections for researchers and whistleblowers, ensuring journalists can conduct investigations without fear of reprisal and threat researchers engaging in responsible disclosure are able to conduct their research. This would encourage more researchers to engage in spyware investigations and provide a legal framework that protects their findings from suppression.

Providing financial support for threat researchers

9 respondents discussed the significant financial burdens associated with effective threat research, and defending researchers in court, that particularly fall on civil society. Respondents proposed to improve the sustainability of the funding model available to threat researchers.

- Respondents mentioned how many civil society organisations and academic institutions engaged in CCICs research lack the financial resources to conduct large-scale forensic investigations. For respondents, by supporting research financially, States could ensure that more organisations have the tools and expertise needed to investigate spyware misuse, through grants and the support of third-party organisations.

Improving technical collaboration and information-sharing relating to threat research on CCICs

20 respondents highlighted the need for greater collaboration and the provision of more technical assistance between Governments, threat researchers, and technology providers, including better sharing of techniques and feedback to maximise the impact of threat research efforts in the market.

- Respondents highlighted the role that technology industry actors had played in enabling the wider threats research landscape, emphasising the importance of both

[8] Publications Office of the European Union. (2024). *Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings ('Strategic lawsuits against public participation')*.
http://data.europa.eu/eli/dir/2024/1069/oj

reports describing the threat landscape that technology firms produce, as well as their broader activity. This includes notifying users who have been targeted by attacks; hardening the security of users' technology, including through 'security by design' policies; taking down accounts associated with threat actors; and bringing lawsuits against irresponsible CCIC vendors.

- Respondents called on technology companies to enhance this support, such as through updating the notification provided to users to ensure they are able to take action and improving long-term support for devices to ensure vulnerable parties are protected through ongoing security updates.

- Respondents also called for more open sharing to and from governments on these threats, such as through a trusted consortium approach, to better direct the efforts of threat researchers. This could include facilitating the sharing of a) CCIC companies being tracked, b) financial relationships c) evidence of irresponsible uses, and d) where research is acted upon.

Responsible Investment

Taking measures to encourage more responsible investment in the CCIC market

5 respondents discussed measures that could be employed by governments, shareholders and / or companies themselves in order to ensure investors are not furthering irresponsible activity.

- Respondents indicated that the issue of the investment landscape funding the wider CCIC market was understudied and should be an area of further exploration, particularly since these investment flows were frequently cross-border so any action would require international cooperation.

- Respondents discussed how investors should employ greater due diligence to ensure they are not funding companies or actors engaged in irresponsible activity. This could be better considered, for instance by including cybersecurity harm in the companies' environmental, social and governance checklists. Investors should apply the UN Guiding Principles on Business and Human Rights through thorough due diligence and human rights impact assessments on all companies they fund – and considering the impact of any technologies or products the company develops

or uses, as well as its supply chain.[9] This could be difficult in practice, because of the opaque nature of the CCIC market and the fact it is often challenging to understand a company's true corporate structure and activity.

- To combat this opacity and the challenges it poses to effective due diligence, some respondents suggested governments should strengthen corporate transparency requirements, including to compel companies to report their beneficial owners.

- However, some respondents highlighted that mandating disclosure of investor information could raise privacy concerns, conflict with the confidentiality agreements often in place in this industry and might deter investment in critical cybersecurity technologies more broadly. Other respondents noted that such disclosures were already required by other mechanisms.

- Some respondents also suggested governments could consider greater investment controls to regulate foreign investment in companies developing or selling CCICs, extending Government security reviews to outbound investments in this sector. However, some respondents highlighted that such controls were complex to implement and enforce.

[9] United Nations Office of the High Commissioner of Human Rights (UN OHCHR). (2011). *UN Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

CONCLUSION

Building on the discussions at the Pall Mall Process conference in February 2024 and earlier discussions at the 2023 Paris Peace Forum, the range of responses collected through this consultation process help highlight the increasing importance and visibility of debate around CCICs, with a variety of views regarding the proliferation and irresponsible use of CCICs provided. Respondents acknowledged the existence of legitimate uses of CCICs; the challenge of constructively shaping industry incentives to promote legitimate and responsible use; the need to respond more actively to irresponsible activity and misuse; and the evolving policy, regulatory, and technical challenges to addressing issues around this market. Responses considered good practices for States and the intrusion industry, alongside the role of threat researchers and investors in shaping / responding to the market and considering how stakeholders can better support the victims of misuse.

The main cross-cutting or framing observations highlighted throughout this report will help to inform the next steps under the Pall Mall Process, including the need for joint efforts surrounding:

- **Recalibrating incentives:** To overcome conflicting incentives, there is a need for agreement on the policies and practices necessary for Governments to shape a more responsible market and ensure responsible use of CCICs. This includes considering the role of cyber capacity building, recognising that many governments share legitimate aspirations to develop their cyber capabilities to enhance their national cyber resilience.

- **Clarifying definitions:** Of scope, and common guiding principles around what constitutes a legitimate and / or a responsible use of CCICs, and appropriate responses to irresponsible activity.

- **Ensuring policy predictability:** As the international regulatory landscape continues to evolve, including as a result of new and emerging technologies, predictability will be key to ensuring an effective joint response.

Based on the discussions of best practice summarised throughout this report, and further dialogue at the 2024 Paris Peace Forum (November 12, 2024), participants in the Pall Mall Process will now cooperate to develop a joint plan of action ahead of the next Pall Mall Process Conference in Paris (April 2025).

ANNEX

Annex A: The Pall Mall Process Declaration

Declaration

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:

1 1.1. **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.

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.

1. 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:

1.1. 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;

1.2 Malware[footnote 1]-as-a-service by which providers develop, maintain, and provide malware to be used against targets on behalf of a customer.

2. 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:

2.1. 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

2.2. 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.

3. The vulnerability and exploit marketplace describes the commercial trade in zero-day vulnerabilities and exploits[footnote 2] that enable cyber intrusion. It does not refer to the commercial payment for vulnerability research to enable cyber defence, such as security testing, or bug bounty programs for cyber defensive purposes.

4. 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.

5. 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.

6. 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.

7. 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.

Annex B: Pall Mall Process Consultation on Good Practices

SECTION 1 – TERMS OF REFERENCE

- This document launches a consultation into good practices through which to tackle the threat presented by the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICS). **Section 1** sets out the process through which this consultation will be run, whilst **Section 2** sets out the questions for different stakeholders to respond to, via the online form that you should have been sent the link to. If you do not have this, please contact us at pallmallprocess@fcdo.gov.uk.

Process

- This consultation will take place under the Pall Mall Process (English/French) – an ongoing international and multistakeholder dialogue to develop joint policy and technical solutions through which to address this shared threat. Led by the Governments of the United Kingdom and France, a coalition of States, businesses and civil society came together in February 2024 to discuss the issue and publish the 'Pall Mall Declaration'.

- The questionnaire below looks to set out a series of guiding questions to inform input from relevant stakeholders under three groups:

- **States** – As regulators and potential customers of the market for CCICs

- **Industry organisations** – involved in and around the market for CCICs, alongside their wider value chain.

- **Civil Society, experts, and threats researchers** – with relevant expertise on the threat presented by the market for CCICs, and responses to it.

- Through this consultation, we invite stakeholders to share views on good practice in response to relevant sections of the guiding questionnaire. This consultation is not an academic exercise, and the questionnaire does not seek perfect examples of the implementation of good practice, nor does it aim to provide definitive solutions to the issue – its purpose is to map existing widespread and varied efforts and good practice across a range of entities. Responding to the questionnaire does not represent a formal commitment to the Pall Mall Process, nor membership of the initiative.

- Whilst this document is addressed to the three stakeholder groups above, we also welcome input from other entities with a relevant interest in the market for CCICs.

Timeframe

- We ask that stakeholders respond to the questionnaire by **11 October 2024**.

- Following this initial consultation period, the responses gathered will be compiled and anonymized by the UK and France for discussion in workshops across the three stakeholder groups. Moderated by third parties, these workshops will look to evaluate, challenge, and compare questionnaire responses.

- Based on questionnaire responses and the workshop discussions, the UK and France will assemble a document to be published as the outcome of this consultation process. This document will be circulated for peer review by the wider Pall Mall community, ahead of a final session to discuss outputs before publication.

Terms

- This consultation does not affect existing obligations of States under customary international law or under international agreements to which they are parties, in particular their obligations under the Charter of the United Nations.

- Responses will only be reviewed by officials from the Governments of the United Kingdom or France. Specific good practices may be highlighted and attributed in the final report, strictly upon formal approval of the quoted stakeholder.

- This document, and engagement through the consultation, is informed by the four guiding 'pillars' of the Pall Mall Process:

  - **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.

  - **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.

  - **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.

- **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.

SECTION 2 – QUESTIONNAIRE ON GOOD PRACTICE

Participants are invited to respond to relevant sections of the questionnaire below, split between questions for States; Industry Organizations; and Civil Society, Threats Research and Academia, via the online form. Please note that answers cannot be longer than 4000 characters (including spaces).

QUESTIONNAIRE ADDRESSED TO STATES

Regional organizations are welcome to provide views on additional good practices within their area.

National frameworks

1. Has your government initiated any reflections on, or released any policies addressing, the risks posed by the transfer and irresponsible use of CCICs?

2. If so, how are the four pillars of the Pall Mall Process declaration (accountability, precision, oversight and transparency) considered within these?

3. Does your State have any existing domestic regulatory legal frameworks that relate to addressing the risk presented by CCICs?

4. How would you define legitimate government use of CCICs? Can you provide examples of this in practice?

5. How would you define responsible government use of CCICs? What are some examples of good practice of this?

Export controls

6. At the national level, what kind of export control measures do you implement regarding CCICs, based on which legal framework?

7. Have you identified any examples of good practice in the implementation of export controls on CCICs?

8. How do you think these export control measures could be made more effective, and / or what challenges do you see?

Procurement requirements

9. At a national level, what processes in place would you recommend as good practice to control or regulate government procurement of CCICs, and / or to ensure minimum standards for 'responsible' activity are met?

10. How do you think these procurement requirements could be made more effective, and / or where do you see challenges?

Skills controls

11. What would you recommend as good practice in the implementation of government skills controls on CCICs?

12. Where are there challenges?

Domestic legal action and support to those impacted by irresponsible activity

13. What legal and / or other mechanisms could your government use or refer to in the event of a suspected irresponsible use of CCICs?

14. What actions could or should be pursued to support those impacted by of commercial cyber intrusion tools and / or services (e.g. technical support, legal action, etc)? Can you provide any relevant examples of good practice?

15. What challenges do you see in taking legal action in this area, including at the international level?

Other good practice:

16. Are there any additional domestic policy levers that your government could potentially make use of to shape the market for CCICs (e.g. transparency measures, import and investment controls etc)? Please provide any examples of good practice.

17. Are there any policy levers that have proved ineffective or counterproductive in tackling the proliferation and irresponsible use of CCICs that you would caution against? If so, why?

18. How can States support efforts by threat researchers to understand the proliferation and irresponsible use of CCICs?

19. Is there anything additional detail on good practice you would like to share regarding the ambitions of the Pall Mall Process?

QUESTIONNAIRE ADDRESSED TO THE INDUSTRY

Organisations working within and around the market for CCICs are invited to provide views on any of the sections below relevant to their area of work.

Organisational process

1. How would your organisation define the responsible development, facilitation, purchase, transfer and use of CCIC products and services?

2. Has your organisation drafted or released any strategies, statements or documents addressing the risks posed by the irresponsible transfer and use of commercial cyber intrusion capabilities?

3. If appropriate, how are the four pillars of the Pall Mall Process declaration (**accountability, precision, oversight, and transparency**) considered in your organisation's approach?

4. Does your organisation have any frameworks, control mechanisms or processes that could support the implementation of these pillars?

Vulnerability marketplace

5. Is your organisation involved in vulnerability research and / or does it interact with vulnerability researchers? If so, how would you define responsible vulnerability research, and what frameworks and / or processes are in place to encourage this?

Managing suppliers

6. Does your organisation implement due diligence mechanisms to manage your cyber intrusion supply chain (including for vulnerabilities / providers)? Can you provide examples of good practice in this area?

7. What, if any, mechanisms does your organisation implement to demonstrate transparency across your cyber intrusion supply chain, and / or provide information on supply chain provenance to customers?

Managing customers

8. Does your organisation take steps to ensure that clients do not participate in the onward transfer of CCICs (through methods such as software licences)? If so, can you provide examples of where this has worked successfully?

9. Does your organisation have internal processes to ensure that your clients do not participate in the irresponsible use of CCICs (such as 'know your customer' practices) or technical measures to improve oversight? If so, what kind of internal processes or technical measures have worked most effectively?

10. Does your organisation recommend any good practices to provide assurance that the end-users of your products and / or services are not using them irresponsibly, such as to undermine human rights?

11. Where irresponsible use is identified, what steps can or should be taken in response?

Other good practice

12. Has your organisation taken any other action not mentioned above to prevent the proliferation and irresponsible use of CCICs?

13. What obstacles do your organisation, or your industry as a whole, encounter when attempting to tackle proliferation and irresponsible use of CCICs? Do you have any suggested solutions to these obstacles?

14. Is there any additional detail on good practice you would like to share regarding the ambitions of the Pall Mall Process?

QUESTIONNAIRE ADDRESSED TO CIVIL SOCIETY, EXPERTS AND THREAT RESEARCHERS

Organisations and individuals involved in threat and cyber security research across industry, civil society and academia are invited to provide views on any of the relevant sections below.

Observing States' good practice

1. What examples have you observed of good practice in responsible state behaviour when tackling proliferation and irresponsible use of CCICs?

2. How do you think they could be made more effective?

3. What new practices should States develop to reinforce their efforts to tackle the proliferation and irresponsible use of CCICs?

Observing good practice across industry

4. What examples have you observed across industry of good practice when tackling proliferation and irresponsible use of CCICs?

5. How do you think they could be made more effective?

6. What new practices should private actors develop to reinforce their efforts to tackle the proliferation and irresponsible use of CCICs?

Supporting threats research

7. What examples have you observed of good practice by threat researchers across civil society and industry in maximising the impact of research into the proliferation and irresponsible use of CCICs?

8. What good practice have you observed in information sharing between organisations to maximise the impact of research into the proliferation and irresponsible use of CCICs?

9. What good practice would you recommend for the process of vulnerability discovery and management, to limit the potential for harmful impact?

10. What challenges have you observed to efforts by threat researchers to understand the proliferation and irresponsible use of CCICs?

11. How can the Pall Mall Process best support efforts by threat researchers to understand the proliferation and irresponsible use of CCICs?

12. Is there any additional detail on good practice you would like to share regarding the ambitions of the Pall Mall Process?

13. What existing research, reporting and initiatives do you consider relevant to tackling the proliferation and irresponsible use of CCICs?