Essential Elements for Ensuring the Industry Guidelines for Commercial Cyber Intrusion Capabilities Deliver on their Potential
Joint Civil Society Submission

17 September 2026

1) Following the adoption of a Code of Practice for States in 2025, the Pall Mall Process, under the leadership of the United Kingdom and France, is currently developing Industry Guidelines on Commercial Cyber Intrusion Capabilities ("the Guidelines"). The Guidelines are expected to be finalized in November 2026. This submission brings together critical perspectives from civil society organisations that have consistently documented the significant harms commercial spyware inflicts on people, communities and institutions, including transnational harms that have profoundly negative impacts across borders and undermine national security, rule of law, and human rights.

2) We appreciate the leadership of the UK and France in advancing this process and their commitment to including civil society in the ongoing negotiations. The Pall Mall Process represents an important first step towards addressing a critical governance gap and provides a foundation for the further development of effective legislative and regulatory measures. **The Guidelines represent a historic opportunity to establish accountability as the expectation rather than the exception in the development, procurement, and use of CCICs, a potential that should not be lost.** We offer this analysis to support States as they enter the negotiations, drawing on our expertise in international law, business and human rights, and the technical realities of the commercial cyber intrusion capabilities (CCICs) industry. It is intended to serve as a practical reference as States work towards a meaningful consensus, while helping ensure that the Guidelines strengthen respect for human rights in the context of CCICs and deliver protections that respond to the realities and experiences of the communities most negatively impacted.

3) We welcome the initial drafts' references to international law and the UN Guiding Principles on Business and Human Rights (UNGPs), which rightly anchor the Guidelines in the existing legal and normative framework governing States and companies in the commercial cyber intrusion market. We encourage the UK and France to retain and strengthen this language. **Building on this foundation, the Guidelines should also recognize the exceptional risks posed by CCICs, given their potential to facilitate grave, irremediable human rights violations and abuses and undermine rights-respecting governance. Exceptional risks demand exceptional restraint, safeguards, and scrutiny.** These risks are not confined to State use, since the proliferation of commercial cyber intrusion capabilities is lowering the barriers for non-State actors to obtain sophisticated intrusive capabilities, with serious consequences for human rights and security. Given the documented and potentially severe harms associated with the misuse of many CCICs, such as spyware or malware, the Guidelines should restrict non-State actors' access to such CCICs. This is particularly important given the inherent difficulty of ensuring meaningful oversight, transparency, and accountability over their development and use by non-State actors. Accordingly, the sale, transfer, or provision of

CCICs to non-State actors should be prohibited where those actors are neither acting on behalf of the State nor conducting digital security research in the public interest. At the same time, States should instead support the work of digital security researchers, including individuals, academic institutions, and civil society, acting in good faith and for the public interest to do vulnerability research and reporting. Furthermore, any use of CCICs must meet the principles of necessity, legality, proportionality, and legitimate aims as established under international human rights law. The Pall Mall Process should set clear standards on the exceptional circumstances under which these technologies can be sold and serviced; and should result in new, robust mechanisms geared at accountability for failing to effectively mitigate the human rights risks embedded within the design of these technologies and affiliated corporate business models.

4) **States' role as users and regulators does not displace companies' independent responsibility to respect human rights, just as companies' responsibilities cannot substitute for States' duties to regulate industry, oversee corporate conduct, and ensure remediation for harms.** For the Guidelines to be a meaningful contribution, they should, at a minimum, translate these existing State obligations and corporate responsibilities into clear requirements and operational expectations for both sets of actors. States and companies negotiating within the Pall Mall Process should refrain from attempts to dilute, reinterpret, or selectively apply these obligations in the name of consensus. Doing so would not be a compromise; it would be a failure of the Process's core purpose, leaving the human rights harms caused by CCICs without remedy.

5) **The Guidelines should make explicit the obligation of States to protect, respect and remediate human rights harms linked to the CCIC industry.** As the Guidelines are intended to be implemented alongside the Code of Practice for States, they should clearly set out the corresponding commitments expected of States, including establishing robust regulatory frameworks, embedding appropriate human rights and risk safeguards in procurement processes, establishing independent oversight of procured companies, and providing adequate and ongoing guidance for companies on compliance. These frameworks should also provide for the identification of companies that present unacceptable human rights risks, including through public registers or other appropriate mechanisms, and establish clear red lines for excluding companies from procurement or suspending and terminating existing contracts. States should develop these frameworks through meaningful multi-stakeholder engagement, including with industry and civil society, while retaining responsibility for setting and enforcing appropriate standards. States should make clear to CCIC actors that the acceptable, law-abiding use of these technologies is narrowly defined and subject to strict limits, rather than determined by commercial expansion or market demand.

6) **The Guidelines should clearly establish the minimum operating requirements, across jurisdictions, for companies developing, provisioning or deploying CCICs, while also articulating evolving best practice.** In line with the UNGPs, companies should be required to identify, prevent, mitigate, and account for the human rights risks and impacts associated with their products, services, business models and value chains. The Guidelines should establish a

clear baseline below which commercial conduct cannot be considered 'responsible', while making clear that alignment with a voluntary code does not in itself demonstrate that a company has fulfilled its human rights responsibilities. The Guidelines can also offer examples of best practices, as well as a framework for companies to progressively strengthen safeguards as risks, technologies, and best practices evolve.

7) **Against this backdrop, the following principles represent the essential elements that the Industry Guidelines should contain.** They are neither aspirational best practices nor an exhaustive catalogue of 'responsible' corporate conduct. Rather, they provide a starting point for translating obligations under international human rights law (IHRL), international humanitarian law (IHL), and the UN Guiding Principles on Business and Human Rights (UNGPs) into more effective regulation of the CCIC industry. The Guidelines should clearly articulate expectations regarding CCIC use (8a), access (8b), procurement (8c), oversight (8d), accountability and remedy (8e), lest they risk legitimising a market that threatens human rights, national security, and the rule of law.

8) States involved in the Pall Mall process should ensure that the Guidelines:
    a) **Set strict, clear limits, grounded in transparent and accessible legal frameworks, on the sale, export, facilitation, and use of CCICs for both States and companies.**
        i) Require that any use has a clear legal basis, serves a legitimate aim, and is necessary and proportionate to that aim, in accordance with applicable IHRL, IHL, and domestic law.
        ii) Identify specific and clearly defined circumstances in which State use may be permissible, while prohibiting uses and technologies that are inherently incompatible with IHRL or IHL.
        iii) Explicitly state that the Guidelines set requirements that all companies are expected to fulfill, and ensure that those requirements are aligned with our recommendations listed below.
        iv) Retain the prohibition of targeting individuals or groups because of their legitimate exercise of human rights or accountability functions, and include a specific reference to journalists, human rights defenders, political opponents, lawyers, judges, academics, and civil society organisations.
    b) **Restrict access to CCICs to actors that meet clear human rights and accountability requirements while protecting legitimate digital security research.**
        i) Prohibit the sale, transfer, or provision of CCICs to non-State actors that are neither acting on behalf of the State nor carrying out digital security research in the public interest.
        ii) Prohibit the sale, transfer, or provision of CCICs to States with a documented pattern of CCICs abuse or inadequate safeguards to prevent abuse.
        iii) Require CCIC companies to assess and continuously monitor the human rights risks associated with customers, intermediaries, suppliers, and other business partners, with heightened scrutiny in conflict-affected and other high-risk settings.

iv) Protect digital security research, including by civil society, academia, and independent researchers, that in good faith and in the public interest identify and responsibly disclose vulnerabilities before they can be exploited.

c) Require robust human rights due diligence prior to and throughout ongoing relationships with CCIC companies.

i) Require States to assess companies' human rights records, ownership and control, business relationships, governance and oversight arrangements, technical and non-technical safeguards, vulnerability-handling practices, and capacity to prevent, detect, and remedy misuse.

ii) Restrict procurement to companies that can demonstrate adequate safeguards and a capacity to meet applicable human rights responsibilities, and establish clear criteria for excluding companies that present unacceptable risks or have failed to address serious abuses.

iii) Require companies to conduct ongoing human rights due diligence consistent with the UNGPs throughout the product lifecycle and across their value chains.

iv) Require meaningful corporate disclosure of human rights due diligence policies, risk assessments, governance arrangements, safeguards, and remediation processes.

d) Require independent and effective oversight of CCIC development, procurement, and use.

i) Establish meaningful authorisation, monitoring, auditing, and review mechanisms, including independent oversight of CCIC companies operating within their jurisdiction.

ii) Require companies to maintain technical and non-technical safeguards that enable effective oversight and facilitate the prevention or rapid detection of misuse, including auditable records of access, legal authorizations and use, license controls, continuous monitoring, and the ability to suspend or terminate access in a timely manner where misuse or abuse is identified.

iii) Establish mechanisms for the responsible disclosure and sharing of vulnerability information with relevant States, civil society and technical experts working on accountability for CCIC-facilitated harms.

iv) Ensure robust protections for whistleblowers and other individuals who report misuse or human rights concerns and require companies to establish appropriate internal mechanisms for whistleblowers and reporting.

v) Prohibit direct and indirect investment, lending, guarantees and other forms of financial support to CCICs companies that are unable to demonstrate alignment with the previous points.

e) Require effective accountability mechanisms and remedy for human rights abuses involving CCICs, including across borders.

i) Require States to translate their obligations under the UNGPs and the Pall Mall Code of Practice into domestic law and effective enforcement frameworks, including across borders.

ii) Require effective avenues to challenge authorizations and provide remedy in relation to the use of CCICs, including by mandating accessible, transparent, and

effective grievance remedy mechanisms, appropriate victim notification, and protection against retaliation.

iii) Require prompt and independent investigation of suspected abuse, effective sanctions and enforcement, and suspension or termination of contracts or access where serious violations are substantiated.

iv) Promote multilateral cooperation and information-sharing to enable States to investigate and hold companies accountable for cross-border misconduct, including through cooperation on investigations, enforcement, sanctions, visa restrictions, export control measures, and access to remedy for affected individuals and communities.

9) **No technology is neutral by default, and some CCICs in particular present heightened and systemic human rights risks that cannot be understood solely through the lens of context or user intent.** Commercial spyware and other targeted surveillance capabilities have repeatedly facilitated arbitrary surveillance and detention, transnational repression, and attacks on heads of state, business leaders, journalists and human rights defenders. An increasing body of litigation, technical analysis, and independent investigations demonstrates that these harms are not exceptional or accidental, but are foreseeable consequences of technologies whose design, business model, and deployment create systemic human rights risks. Recognising these systemic risks is therefore essential to ensuring that the Guidelines can deliver meaningful protection in practice.

10) **The utility of the Guidelines will depend not only on their substantive commitments, but also on the integrity of the process through which they are developed and implemented.** While we appreciate the efforts made thus far to broaden participation by including a range of perspectives at the table, including civil society, academia, independent technical experts, and investigative laboratories, civil society participation in the negotiations should be more systematic, sustained, and substantive. The process should also ensure meaningful engagement with individuals and communities directly affected by the misuse and abuse of commercial spyware at every key stage of the Guidelines' development and implementation.

11) **At the same time, the process should be driven by actors with a demonstrated commitment to human rights, human rights-based governance, and demonstrably strong, independent mechanisms to ensure rights-respecting deployment of surveillance technologies.** Given the importance of this process, the participation and influence of entities that fall short of these standards risks undermining the integrity of both the process and its outcome. Those wishing to engage in Pall Mall with a documented record of causing, facilitating or profiting from serious human rights abuses should be received with heightened scrutiny and with reservations. In particular, companies and individuals subject to sanctions or credibly linked to repeated abuses involving CCICs should not shape the standards by which the industry will be judged. Instead, the Guidelines should establish new and higher standards rather than codifying the status quo.

12) We look forward to deepening our engagement in the next stages of this process and to working together to ensure that it is supported by the time, resources, and sustained attention needed to develop Guidelines that are both meaningful and effective. We are confident that, through this collective effort, we can deliver Guidelines commensurate with the importance of what is at stake.

Signed,

Organizations:
Business and Human Rights Centre
Freedom House
Amnesty International
Centre for Democracy and Technology Europe
Access Now
Resident NGO
Human Constanta
Digital Rights Foundation
Institute for Policy Research and Advocacy (ELSAM)
Hiperderecho
CyberHUB-AM Threat Lab
Data Rights
Human Rights Defence Centre
TechMOV
Tech Global Institute
Fundación Acceso
IPANDETEC
Heartland Initiative
Protect.ngo
Economic Security Council of Ukraine
Conexion Segura y Libre (CSL)
Association for Progressive Communications (APC)
Ranking Digital Rights
Privacy International
Fundación Karisma

Individual experts:
Lisandra Novo, Senior Law & Tech Advisor
Ragheb Ghandour, Technical expert
Hinako Sugiyama, International Justice Clinic at the University of California, Irvine School of law