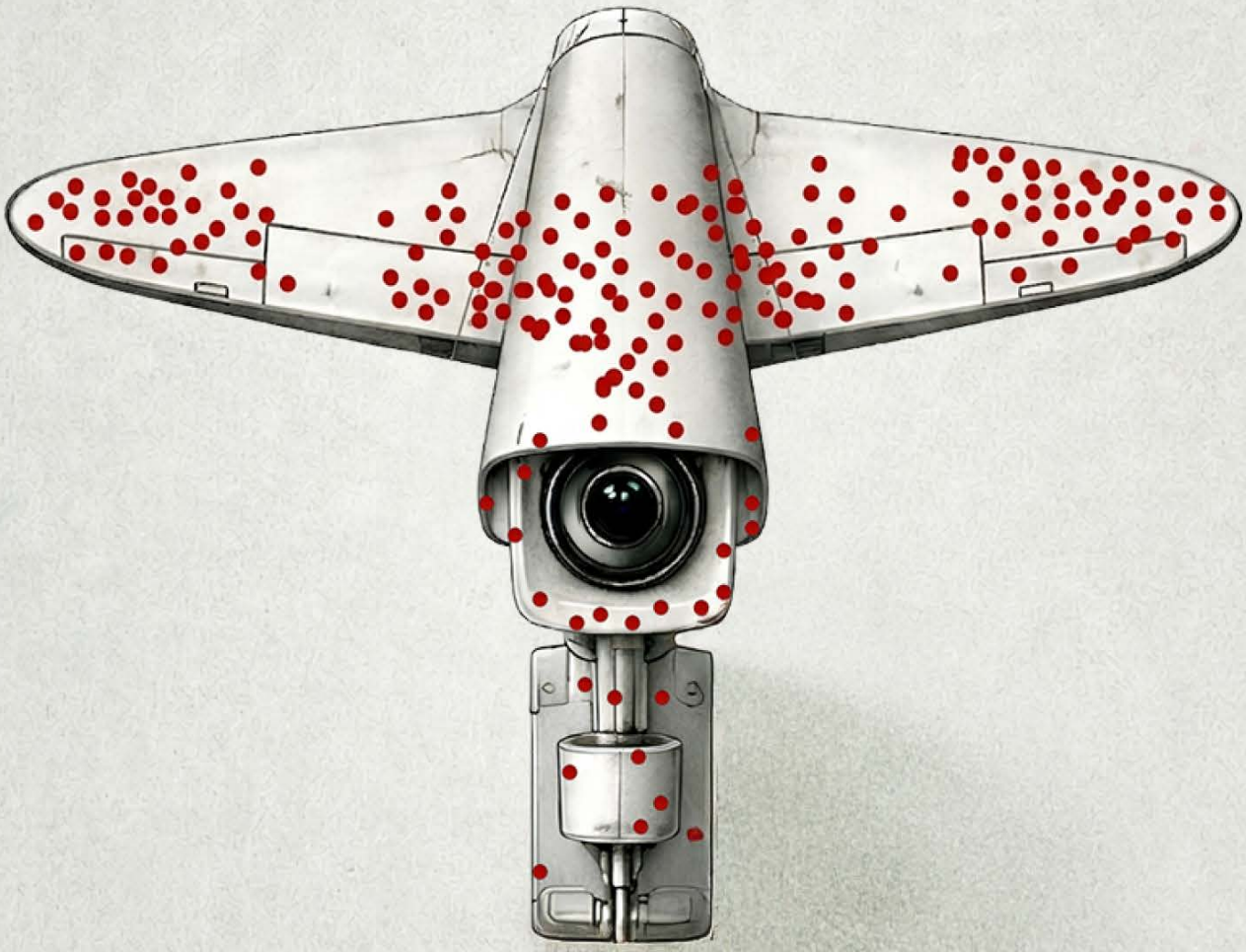
SPYWARE BIAS

The Security Shortfall in Norms-Based Governance



ECONOMIC SECURITY COUNCIL *of* UKRAINE

RADA
VERKHOVNA RADA OF UKRAINE

SPYWARE BIAS

THE SECURITY SHORTFALL IN NORMS-BASED GOVERNANCE

EXECUTIVE SUMMARY

Efforts to govern commercial cyber intrusion capabilities (CCICs) through norms-based initiatives have gained traction among like-minded states, yet their capacity to deliver security outcomes remains unproven amid asymmetric threats.

Initiatives like the Pall Mall Process (PMP) explicitly frame their objectives in security terms, launching to "tackle the challenges posed by the proliferation and irresponsible use of [CCICs]" whose "irresponsible use [impacts] national security," and committing states to "mitigate the threats" through pillars of accountability, precision, oversight, and transparency[1]. This analysis evaluates PMP—now endorsed by over 27 states including the US, EU members, UK and Japan—against four criteria: participation scope, constraint mechanisms, threat alignment, and observable security effects. While PMP consolidates normative consensus among compliant consumers, it engages only one major production hub (Italy) while 21 of 31 high-risk vendors operate in non-aligned jurisdictions like Israel and India.

Participation skews toward states already inclined to restraint, leaving principal threat vectors like state-centric export discretion in supplier hubs and unchecked proliferation beyond reach. Voluntary commitments yield no binding costs, as evidenced by post-PMP persistence: Pegasus targeting Serbian journalists (2025), an expanding $55 billion surveillance market (2025 projection, tripling by 2033), and rising private capital in offensive cyber firms.

INTRODUCTION

Efforts to regulate the commercial spyware market are gaining momentum, with initiatives like the Pall Mall Process seeking to curb the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICs). The continued rise of awareness on this issue on an international level reflects a growing concern that unchecked diffusion of intrusive cyber tools poses risk not only to human rights, but to national security and digital stability. At their core, initiatives aiming to regulate the spyware market, like the Wessanaar Arrangement, Pall Mall Process, EU dual-use regulation etc., rely on norms-based governance models intended to shape state and market behaviour in the absence of binding regulation.

Commercial cyber intrusion tools have become widely accessible and are now one of core mechanisms in the intelligence and security practices of dozens of states. Faced with rapid technological change and limited appetite for formal regulation, European governments and their partners have turned to voluntary commitments as a pragmatic response.

There is, however, a big question of the effectiveness of this approach, seeing as the actors most frequently associated with production and coercive or abusive uses of CCICs are often states and proxies operating outside voluntary governance arrangements. By contrast, participation in norms-based initiative is concentrated among countries that are already inclined toward regulatory compliance and, in many cases, lack significant domestic production of offensive spyware. As a result, governance efforts risk constraining those already inclined toward compliance, while leaving the principal sources of threat untouched.

[1] https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states

Non-binding design stems from the aim to prioritize consensus among like-minded governments over adversarial leverage, which effectively renders it ineffective against primary misusers. Most of what voluntary norms can do in this context is avoid alienating potential adopters but they fail in asymmetric threats, where hostile actors ignore reputational pressure.

There is little doubt that the appeal of norms-based governance lies in its low political cost and its capacity to demonstrate engagement in a difficult policy area. It offers governments a way to respond to growing concern without committing to enforcement mechanisms that are often costly and exceptionally slow compared to the rapid developments of the spyware market. In the cyber domain, however, the absence of binding obligations raises a more consequential question of whether voluntary restraint can plausibly influence behaviour in a market largely shaped by competition and uneven incentives. Where governance does not impose measurable costs, does not require behavioural adjustment, and does not reach the actors most responsible for misuse, its contribution to security cannot be assumed. The central issue, therefore, is not the normative appeal of such initiatives, but whether they materially alter exposure to cyber intrusion risks or simply institutionalise restraint among those already predisposed to comply.

Purpose

This research evaluates whether current norms-based approaches to governing CCICs function as effective security instruments. Using European-led initiatives as a reference point, it assesses whether voluntary restraint meaningfully reflects a positive shift in the CCIC market or reduces exposure to cyber espionage and coercive surveillance in an increasingly adversarial digital environment.

METHODOLOGY

The research turns to qualitative comparative analysis to assess whether norms-based governance of CCICs produces meaningful security outcomes. It applies a structured set of four evaluative criteria:

First, participation scope. The research examines which states and market actors are encompassed by a given governance framework and which are not.

Second, constraint mechanisms. The research assesses how governance frameworks impose restraint in practice, whether through legal obligation, economic cost, reputational pressure or political signalling.

Third, threat alignment. The research tests whether governance frameworks bind the actors most responsible for CCICs misuse.

Fourth, observable security effects. Security outcomes here refer to measurable reductions in exposure to cyber intrusion risks, including lower incidence of unauthorized targeting and espionage against state institutions or coercive surveillance of civil society, constrained market proliferation through vendor exits or relocation, and diminished misuse by high-risk actors.

Empirically, the methodology combines document analysis of governance frameworks with open-source reporting and selected case illustrations. The PMP serves as the primary case study, while the Wassenaar Arrangement and EU Dual-Use Regulation are used as a limited comparator to test whether more formalised control regimes overcome the same structural constraints.

Policy implications and contribution

The research suggests that norms-based governance, in isolation, is poorly suited to an environment characterised by asymmetric incentives and adversarial behaviour. The contribution of this study lies in reframing CCICs governance as a question of strategic effectiveness rather than normative aspiration. It offers policymakers a clearer basis for assessing whether existing approaches enhance security or merely signal virtue in a market and threat landscape that continues to evolve regardless.

WORKING DEFINITIONS

The PMP adopts deliberately broad terminology, allowing for the definitions to be shaped throughout the process. The first annex of its declaration[2] refers to CCICs as "tools and services offered by intrusion companies that enable unauthorised access to, or interference with, computer systems." This umbrella concept encompasses both products and operational services, including access-as-a-service (ACaaS)—where a provider supplies the access vector—and malware-as-a-service (MaaS)—where a company develops and maintains intrusive software deployed against a target on behalf of a client. PMP further defines cyber intrusion companies as commercial business entities that sell "off-the-shelf" penetration tools, vulnerabilities, exploits, or hacker-for-hire services for profit.

For the purposes of this policy brief, that scope is narrowed deliberately. While the PMP framework includes both capability vendors and operational contractors—often described as "hackers-for-hire"—this work focuses exclusively on firms that develop, license, and maintain commercial intrusive surveillance software. In other words, ***the subject of examination is commercial spyware vendors (CSV): companies that produce scalable intrusion platforms capable of remote device compromise, data extraction, and persistent surveillance, whether delivered through direct licensing or as a managed technical service.***

This is a methodological distinction that allows for further analysis in this sphere of other types of vendors and CCICs. Hackers-for-hire operate through bespoke, case-by-case intrusion campaigns that rely heavily on operational tradecraft. Commercial spyware vendors, by contrast, industrialise intrusion capability. Their products can be exported, replicated, updated, and redeployed across jurisdictions, creating structural proliferation risks that are more susceptible—at least in theory—to export controls and market-shaping governance mechanisms. Because this brief evaluates the efficacy of norms-based and export-control regimes, it concentrates on the segment of the ecosystem most directly affected by licensing, dual-use classification, and cross-border transfer controls.

Accordingly, when this paper refers to CCICs, it does so within the PMP's definitional architecture but applies the term in a confined sense: products of companies engaged in the development and commercialisation of spyware delivered through ACaaS and MaaS models.

ON COMMERCIAL SPYWARE

The market for CCICs operates in a space exceptionally difficult to map. Not only are the products and services for sale digital, but they are also inherently dual-use: the same capability can ensure lawful intelligence collection or enable coercive surveillance, depending entirely on who acquires it and for what purpose. Intent, for that matter, is not inherent in the technology itself but deferred to the end user.

This ambiguity shifts the burden of responsibility upstream. Governments that host or license commercial spyware firms are not always in a position to determine how a tool will ultimately be deployed, yet their approval processes shape which capabilities enter

[2] https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

circulation and under what conditions. In the absence of enforceable safeguards, this structure relies heavily on assumptions of responsible use — assumptions that have repeatedly proven fragile in practice.

The analytical challenge is further compounded by the limited visibility of the market itself. At the time of writing, the PMP has not published a definitive list of CSV within the scope of its governance efforts. As a result, this research draws on three publicly available and independently produced sources to identify relevant actors: the Atlantic Council's *Mythical Beasts* report[3], Google Threat Analysis Group's *Buying Spying*[4], and the European Parliament's *PEGA Investigation into the use of Pegasus and equivalent surveillance tools*[5]. Taken together, these sources provide the most credible open-source picture of the sector, despite inevitable gaps.

It is also important to delimit what is—and is not—being assessed. The CSV examined here are primarily those developing spyware tools designed for remote access and device compromise. While "commercial spyware" is often used as a "catch-all" term, the market broadly divides between systems intended for lawful interception and data retention, and those engineered to covertly penetrate devices and extract data. This analysis is concerned almost exclusively with the latter category, commonly described as offensive cyber capabilities. References in this paper to CSV, state use, or proliferation therefore pertain to this subset, as consistently classified by the Atlantic Council, Google TAG, and the PEGA inquiry.

PARTICIPATION SCOPE

The initial Pall Mall Conference gathered 27 states and international organisations, 14 industry and 12 civil society and academia representatives. Out of 53 entities 27 states signed the Code of Practices. Among the state signatories, nearly all have documented histories of purchasing or using CCIC, with the notable exceptions of Kosovo and Norway. At the same time, only a subset of participating states play a structural role in the spyware ecosystem itself. Seven signatories—France, Germany, Greece, Hungary, Ireland, Italy and the United States—are found to be hosts of CSV or elements of their operational infrastructure identified in this research. The remaining participants engage primarily as consumers or norm entrepreneurs, rather than as nodes of production.

This distribution becomes more consequential when set against the broader geography of supply. SIPRI's mapping identifies forty-three spyware manufacturers operating across eighteen states, with production far more concentrated than in adjacent cyber-surveillance sectors.[6] Over half of these firms are located in just three countries: India, Israel, and Italy. Similarly, the Atlantic Council also draws attention to this structural imbalance through its identification of the same three countries —"The three I's"— as central hubs of commercial spyware production.[7] Drawing on open-source investigations, this study identifies 31 CSVs that routinely emerge as risk factors in the spyware market. Consistent with both SIPRI's and the Atlantic Council's findings, a substantial majority are Israeli firms: Blue Ocean, Candiru, Cellebrite, Cognyte, ClearTrail, Interionet Systems, Merlinx, NSO Group, Paragon Solutions, QuaDream and Wintego Systems. A second cluster is based in India, accounting for three companies (as most Indian CSV provide hack-for-hire services), followed by smaller clusters in the UAE, Cyprus, Turkey, Russia, Vietnam and Singapore.

The implication is difficult to ignore. **Twenty-one out of the thirty-one vendors** most closely associated with spyware proliferation operate in jurisdictions that fall entirely outside the PMP. These firms—and, by extension, the states that license or tolerate them—remain largely insulated from the reputational and normative pressures the initiative is

[3] https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them/
[4] https://blog.google/threat-analysis-group/
[5] https://www.rcmediafreedom.eu/Resources/Reports-and-papers/PEGA-Committee-final-report
[6] https://www.sipri.org/publications/2025/other-publications/export-controls-and-spyware-enhancing-oversight-transparency-and-restraint
[7] https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/

designed to generate. As a result, participation aligns more closely with patterns of consumption and compliance than with the supply and development that shape the market's most consequential dynamics.

COMPANY	TYPE	SPYWARE PRODUCT	HOSTSTATE
1Byte	Developer	Spyware/Stalkerware TheTruthSpy	Vietnam
9th Vision	Developer	Zero-Click Spyware/Surveillance	South Africa
Aglaya	Developer	Spyware/Surveillance Cyber Strike	India
Blue Ocean	Developer	Offencive Spyware	Israel
Candiru (Saito Tech Ltd)	Developer	Spyware DevilsTongue	Israel
COSEINC	Developer	Spyware/Surveillance	Singapore
Cognyte	Developer	Spyware/Surveillance	Israel
CY4GATE	Developer	Spyware/Surveillance Epeius, Hydra	Italy
RCS Lab	Subsidiary (CY4GATE)	Spyware/Surveillance Hermit	Italy
CPX (DarkMatter)	Developer	Spyware/Surveillance Project Raven	UAE
Interionet Systems	Developer	Spyware/Surveillance NightHawk	Israel
InvaSys	Developer	Spyware/Surveillance Invasys Mobile360	Czech Respublic
Intellexa Consortium	Web of CSV	Spyware/Surveillance	Greece
Cytrox	Developer	Predator	North Macedonia
			Hungary
Nexa Technologies	Developer	Cerebro	France
Thalestris Limited	Distributor	Predator	Ireland
Trovicor (Data Fusion)	Developer	Spyware/Surveillance	Germany
Cellebrite	Developer	Spyware Universal Forensic Extraction Device (UFED)	Israel
ClearTrail Technologies	Developer	Spyware Astra	India
Leo Impact	Developer	Spyware/Surveillance	India
MerlinX	Developer	Apollo	Israel
Negg Group	Developer	Vbiss	Italy
Nexa Technologies	Developer	Spyware/Surveillance Cerebro	France
NSO Group	Developer	Pegasus	Israel
Paragon Solutions	Developer	Graphite	Israel
			USA
PARS Defence	Developer	Spyware/Surveillance	Turkey
Passitora	Developer part of the Intellexa Alliance	Surveillance	Cyprys
Positive Tecnologies	Developer	Spyware/Surveillance Provide data to FSB and GRU	Russia
QuaDream	Developer	Reign	Israel
InReach	Distributor		Cyprys
Wintego Systems	Developer	Helios	Israel (ties to Singapore)

Information about current statuses of CSVs, their host countries and activity was verified through Surveillance Watch https://www.surveillancewatch.io/entities

CONSTRAINT MECHANISMS

As stated in its Code of Practices, PMP is explicitly voluntary and non-binding.[8] It promotes good practices across four pillars (accountability, precision, oversight, and transparency) but imposes no legal obligations or penalties on neither the participants nor outsiders.

The official documents outline aspirational tools like national export controls, procurement restrictions on irresponsible vendors, human rights due diligence, and international cooperation for sanctions or debarment. These depend on domestic implementation by states and mainly encourage self-reporting and information sharing. No mechanisms exist to bind non-participating states or actors that host CCICs, as the process targets proliferation through moral responsibility rather than enforcement.

Similarly to PMP, Wassenaar Arrangement (WA) features no binding constraints, relying on voluntary national implementation. Member countries retain full control over national implementation, limiting utility against CCIC proliferation and misuse.

WA operates through two main control lists—its Dual-Use Goods and Technologies List and its Munitions List—with certain items within the Dual-Use List designated as "Sensitive" or "Very Sensitive" to ensure higher scrutiny on exports.[9] The Munitions List includes conventional arms-related items, while the Dual-Use List encompasses, among other technologies, cyber intrusion software subject to those higher-scrutiny tiers. Participating states commit to annual (and in some cases semi-annual) reporting on transfers, license denials for certain controlled dual-use items—including those in the Sensitive and Very Sensitive categories—and end-use assurances. Denial notifications are circulated among members so as to inform others and prevent circumvention by routing through less restrictive jurisdictions. These arrangements are then reinforced through annual Plenary meetings that harmonize the lists and promote common best practices, although enforcement remains entirely national, with no WA-level verification mechanism or supranational penalties.

THREAT ALIGNMENT

The European Union has sought to rein in spyware proliferation through its export control regime by classifying certain cyber-surveillance technologies as dual-use items under the Dual-Use Regulation. Under this framework, technologies that could enable covert surveillance are subject to export authorisation controls designed to prevent transfers that risk "internal repression" or serious human rights violations. Yet this dual-use framing carries its own limitations: by equating spyware with broadly defined civilian and military applications, the regulation places primary authority over risk assessment with national governments, which retain discretion over licensing and end-use determinations. As a result, export controls often reflect state-centric security considerations and commercial interests more than consistent human rights safeguards. The practical effect is a patchwork of implementation across member states, with varied enforcement standards and regulatory loopholes that allow spyware to flow through the Union's internal market and beyond, despite longstanding evidence of misuse documented by independent investigations.[10]

As established above, neither PMP nor WA or the EU Dual-Use Regulation for that matter, create binding legal obligations. For the threat states outside these arrangements initiative-led restraint and oversight remain absent altogether. So structurally, they sit beyond the effective reach of Pall Mall–oriented constraint.

For some even alignment on paper does not necessarily translate into restraint in practice. Though not a member of the WA Israel, for example, has publicly committed to aligning its export controls with WA standards. In practice, licensing decisions are administered

[8] https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states
[9] https://www.wassenaar.org/control-lists/
[10] https://vtechworks.lib.vt.edu/items/8d3a485d-3470-4976-bc44-82e538b47d14

through the Defense Export Controls Agency (DECA) within the Ministry of Defense under the 2007 Defense Export Control Law. Sales have been blocked when perceived to conflict with Israeli national interests—for instance, denials of Pegasus exports to Ukraine and Estonia to avoid diplomatic friction with Russia.[11] This demonstrates that export controls can function decisively when strategic priorities are implicated.

Yet the pattern of documented abuse suggests that national interest filtering does not always equate to human rights filtering. NSO Group has publicly committed to alignment with the UN Guiding Principles on Business and Human Rights. Nonetheless, forensic investigations by Amnesty International and Citizen Lab have repeatedly documented Pegasus deployments against journalists, opposition figures, and civil society actors. Cases span multiple jurisdictions and political contexts: journalists in Serbia targeted in 2025[12]; repeated targeting of Indian media figures in 2023–2024[13]; surveillance linked to the associates of Jamal Khashoggi[14]; investigations in Mexico, Hungary, and Morocco[15]; and the 2021 Pegasus Project, which identified more than 180 journalists globally as potential targets[16].

The issue is not simply that misuse persists. It is that existing alignment mechanisms operate through state-centric export discretion rather than systemic market discipline. Controls may be applied selectively, often in response to geopolitical considerations, while remaining permissive toward clients whose conduct generates reputational cost but limited strategic friction.

A similar dynamic is visible beyond the Israeli ecosystem. India classifies offensive cyber tools as dual-use items under its SCOMET control list, placing final export authority in the hands of the Directorate General of Foreign Trade (DGFT). Companies may initiate and structure sales, but every international transfer requires a government license. Approval is contingent on review by an inter-ministerial working group, which assesses whether the transaction aligns with India's national security and diplomatic interests.

On paper, this mirrors the architecture of responsible export control. In practice, it reinforces the same structural dynamic as seen with Israel where discretion rests with the state, and the decisive criterion is strategic alignment rather than external oversight.

As for the other states, Russia's System for Operative Investigative Activities (SORM) has been exported to neighboring states and partners in Central Asia and Latin America, embedding surveillance capabilities at the ISP level and enabling population-scale monitoring without device-level compromise. China has promoted Huawei-linked "Safe City" systems across several African capitals, integrating urban surveillance infrastructure into broader digital governance packages. At the same time, China supports a substantial vulnerability research ecosystem, accounting for roughly 30 percent of detected zero-days in 2024.[17]

Even though these models differ technically from Western-origin remote access tools, collectively they normalize the integration of offensive or intrusive capabilities into statecraft. Once again, many of these suppliers operate outside Pall Mall's normative perimeter. As a result, threat production and proliferation are concentrated in jurisdictions where governance initiatives exert limited leverage.

So when it comes to threat alignment, even in states that maintain structured export regimes and nominal adherence to multilateral standards, restraint is mediated through national interest. Normative alignment does not automatically translate into human rights alignment. And where governance remains discretionary and opaque, voluntary international processes have limited leverage over the actors most capable of shaping the market's risk profile.

[11] https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia
[12] https://www.amnesty.org/en/documents/eur70/9186/2025/en/
[13] https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/
[14] https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-jamal-khashoggi-wife-phone-washington-post/
[15] https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/
[16] https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware
[17] https://www.recordedfuture. bhy6tgcom/research/pegasus-pall-mall-managing-risks-of-offensive-cyber-capabilities

OBSERVABLE SECURITY EFFECTS

If norms-based governance is to be judged seriously, it must be judged against observable change. On that metric, the record remains thin. The CCIC market is opaque by design with solid evidence of shift rarely surfacing in real time. Yet the absence of this evidence cuts both ways. At the time of writing, there are no verifiable indicators of neither market contraction, structural vendor exit/relocation, nor measurable reduction in targeting patterns attributable to PMP. Participation has not generated identifiable behavioural shifts that would plausibly correlate with reduced exposure or improved security for signatories.

Nonetheless, what can be observed instead is continuity. The global surveillance market is projected to expand significantly over the coming decade, with growth driven by demand for CCICs. It is already projected at $55.03B in 2025 and is expected to reach $168.71B in 2033;[18] The global cyber security services market size was valued at $75.82B in 2024 and is projected to reach $156.76B by 2030, growing at a CAGR of 13.6% from 2025 to 2030, reflecting arms race fueling spyware.[19]

There is also vast evidence of increased funding in the market exemplified by sharp increase of private capital flows into surveillance technology, with U.S. investors backing a growing number of firms involved in offensive cyber capabilities. This surge positions the US as the largest national investor in commercial spyware, surpassing Israel (26 investors), Italy (12), and the UK (5). For that matter it is capital expansion that defines the post-Pall Mall environment.[20]

Targeting activity also continues in jurisdictions aligned with norms-based initiatives. Investigations by Amnesty International's Security Lab confirmed that NSO Group's Pegasus spyware was used to target investigative journalists in Serbia after the launch of the PMP. Separate reporting by the Associated Press and Citizen Lab documented the deployment of Israeli-developed spyware against Italian journalists amid domestic political scrutiny.[21] Not to say that these cases establish causation between governance and harm, but they do underscore the absence of a detectable deterrent effect.

In policy terms, the absence of observable security dividends is itself an outcome.

Voluntary governance has not demonstrably reduced the operational tempo of high-risk spyware deployment, nor has it altered the structural incentives driving production and export. If governance mechanisms are designed to influence the proliferation in this market their effectiveness must ultimately be assessed against measurable change. At present, such change is not evident.

CONCLUSION

This policy paper examined whether norms-based governance mechanisms—centred on the Pall Mall Process—can meaningfully constrain the proliferation and misuse of commercial spyware. It assessed participation scope, threat alignment, export-control architecture, and observable security effects across key supplier jurisdictions. The paper finds that while the PMP has articulated shared principles and consolidated a coalition of signatory states, major production hubs remain outside its perimeter, export licensing of which remains discretionary and state-centric. Moreover, no observable proxies— those among market contraction, reduced targeting patterns, or measurable protection gains for participants—indicate systemic behavioural change. Meanwhile, the global surveillance market continues to expand, private capital investment in offensive cyber firms is increasing, and documented spyware targeting persists in both aligned and non-aligned

[18] https://www.marketresearch.com/Maia-Research-v4212/Global-Surveillance-Trends-Forecast-Broken-43901024/
[19] https://www.grandviewresearch.com/industry-analysis/cyber-security-service-market
[20] https://www.debugliesintel.com/global-spyware-market-2025-us-investment-surge-and-broker-enablers-fueling-proliferation-risks/
[21] https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware/

jurisdictions. The principal implication, therefore, is not that norms are irrelevant, but that their current configuration has not altered the structural drivers of proliferation.

From this perspective, the observed structural limitation is mostly geopolitical. Normative coalitions operate most effectively where supplier states are politically aligned and commercially integrated. Yet the spyware market itself is not geographically neutral. Key production hubs, capital flows, and high-risk end-users sit both inside and outside the normative perimeter. As a result, voluntary commitments discipline only a portion of the ecosystem.

This dynamic carries second-order consequences that merit attention. By consolidating compliant, largely European and transatlantic states around shared standards, initiatives such as PMP may contribute—unintentionally—to a market division. One segment of vendors will prioritise continued access to regulated markets, adapting corporate governance structures and transparency practices accordingly. For these firms, alignment with norms will present a competitive advantage.

A parallel segment, however, may rationally conclude that commercial opportunity lies elsewhere. Vendors less concerned with reputational exposure—or operating in jurisdictions beyond the reach of coordinated export control—may orient toward clients in regions where transparency demands are weaker and procurement decisions are driven primarily by regime security considerations. In this scenario, the most permissive parts of the market become more permissive still. Rather than managing the global spyware ecosystem, this type of regulation could redistribute it.

The long-term implication lies in a notion that a polarised market risks deepening technological divides between regulatory blocs. States operating within norms-based frameworks may impose tighter licensing and oversight, while others consolidate advanced surveillance capabilities without comparable constraints. This divergence complicates human rights protection, undermines collective responses to transnational cyber threats, and may entrench asymmetries in digital power projection. It also makes future multilateral harmonisation more difficult, as regulatory philosophies and industrial ecosystems drift apart.

A crucial notion here is that none of this renders norms-based governance irrelevant. On the contrary, the Pall Mall Process demonstrates that political coordination on commercial cyber intrusion is possible. But coordination alone does not equal constraint. Without broader supplier alignment, stronger transparency mechanisms, and clearer accountability structures, voluntary initiatives risk stabilising a divided market rather than reshaping it.

Therefore, ahead lies a big strategic challenge. If the objective is to reduce misuse and enhance security, governance efforts must anticipate market adaptation and geopolitical fragmentation. Otherwise, well-intentioned norms may harden the very fault lines they seek to bridge.

RECOMMENDATIONS

To strengthen the Pall Mall Process as a meaningful instrument against CCICs proliferation and misuse, states should operationalize its four pillars through targeted, feasible actions. These recommendations build directly on the PMP Code of Practice, addressing identified gaps in voluntary norms by introducing enforcement tools, capacity-building, and multistakeholder verification.

PILLAR 1

ACCOUNTABILITY

Accountability demands rigorous adherence to international law, UN norms, and domestic controls, yet current PMP commitments engage compliant states while major exporters operate unchecked.

Recommendation 1

Participating states should require **mandatory registration of domestic CCIC vendors**, including disclosure of corporate structure, export jurisdictions, and due diligence procedures. Licensing approvals and denials should feed into a secure PMP-wide database to map proliferation patterns and identify recurring risk indicators.

Such registries would not expose sensitive operational details but would create a shared baseline of market visibility, reducing regulatory arbitrage and enabling cross-state comparison of export practices.

Recommendation 2

PMP states should develop a coordinated **sanctions playbook** for entities demonstrably linked to severe CCIC misuse. Leveraging existing UN General Assembly resolutions on spyware misuse can provide normative cover for multilateral alignment.

The objective is to impose tangible reputational and economic costs on repeat offenders, thereby deterring vendor relocation strategies that exploit jurisdictional gaps.

PILLAR 2

PRECISION

Precision requires proportionate, targeted CCIC deployment for lawful purposes, countering the spyware market's evasion via SaaS models and zero-days.

Recommendation 3

Participating states should codify **necessity and proportionality tests specific to CCIC deployment**, explicitly prohibiting targeting of journalists, political opposition, and civil society. Pre-operation collateral risk assessments—particularly for infrastructure-level tools—should become mandatory.

This would embed human rights thresholds directly into operational decision-making rather than relying solely on post hoc review. The goal is to establish human-rights checks as a required step before any intrusive cyber operation, especially those that could harm civilians, journalists, or critical infrastructure.

Recommendation 4

Develop shared PMP **training modules and workshops**. Capacity-building efforts should prioritize the countries with emerging cyber-procurement markets, so that weaker or newer players do not become “governance gaps” while more advanced states tighten their rules.

By doing this, PMP could raise professional standards across the board, making it harder for CCIC misuse while still allowing law-enforcement and national-security operations to continue.

PILLAR 3

OVERSIGHT

Oversight calls for independent audits and resourcing, but lacks teeth against non-participants, perpetuating enforcement gaps.

Recommendation 5

States should establish or designate **autonomous oversight authorities** with technical expertise and civil society representation to review high-risk CCIC exports and domestic deployment authorisations. These bodies must have access to classified assessments and the authority to issue recommendations.

Embedding technical and rights-based review at the approval stage enhances credibility and reduces politicised decision-making.

Recommendation 6

States should require systematic after-action **reviews of CCIC deployments**, including compliance verification and documented lessons learned. By publishing regular aggregated summaries, states strengthen oversight across PMP without heavy costs.

This creates a clear record of each operation's conduct, helping governments spot patterns of misuse or errors without revealing sensitive information to the public.

PILLAR 4

TRANSPARENCY

Transparency promotes information sharing on vendors and threats, yet opacity shields non-signatories fueling the market.

Recommendation 7

Create a secure clearinghouse for **anonymised reporting of spyware incidents**, vendor activity patterns, and suspected misuse cases. Partnerships with technical NGOs and cybersecurity firms would allow independent validation and human rights impact assessment.

Aggregated analysis would support evidence-based policymaking and early-warning detection of proliferation hotspots.

Recommendation 8

Impose **"know your vendor" and “know your customer”** procurement rules to conduct enhanced due diligence on vendors, including beneficial ownership verification, compliance history checks, and contractual clauses enabling termination upon misuse. Reporting on export denials and procurement suspensions would spotlight systemic risk patterns.

Demand-side discipline is often more powerful than export-side control; procurement reform shifts leverage toward responsible vendors.

ACTOR	TYPE	GOVERNANCE STATUS	CCIC ROLE	DOMESTIC VENDOR
African Union	International organisation	Participant	-	
Australia	State	Participant	Purchaced/Used	
Austria	State	Signatory	Purchaced/Used	
Belgium	State	Signatory	Purchaced/Used	
Canada	State	Participant	Purchaced/Used	
Czech Respublic	State	Participant	Purchaced/Used **Host**	**InvaSys**
Denmark	State	Signatory	Purchaced/Used	
Estonia	State	Signatory	Purchaced/Used	
Finland	State	Signatory	Purchaced/Used	
France	State	Signatory	Purchaced/Used **Host**	**Nexa Technologies**
Germany	State	Signatory	User (Pegasus) **Host**	
Ghana	State	Signatory	Purchaced/Used	
Greece	State	Signatory	Purchaced/Used **Host**	**Intellexa**
Gulf Cooperation Council	International organisation	Participant	-	
Hungary	State	Signatory	Purchaced/Used **Host of the operational infrastructure**	**Intellexa**
Ireland	State	Signatory	Purchaced/Used **Host of the operational infrastructure**	**Intellexa**
Italy	State	Signatory	Purchaced/Used **Host**	**CY4GATE**
Japan	State	Signatory	Purchaced/Used	
Kosovo	State	Signatory	-	
Latvia	State	Signatory	Purchaced/Used	
Luxembourg	State	Signatory	Purchaced/Used	
Malaysia	State	Participant	-	
Moldova	State	Signatory	-	
Netherlands	State	Signatory	Purchaced/Used	
New Zealand	State	Participant	Purchaced/Used	
Norway	State	Participant	-	
Poland	State	Signatory	Purchaced/Used	
Republic of Cyprus	State	Participant	**Host of the operational infrastructure**	**Passitora QuaDream**
Republic of Korea	State	Signatory	Purchaced/Used	
Romania	State	Signatory	Purchaced/Used	
Singapore	State	Participant	Purchaced/Used **Host**	**COSEINC**
Slovakia	State	Signatory	Purchaced/Used	
Slovenia	State	Signatory	Purchaced/Used	
Sweden	State	Signatory	Purchaced/Used	
Switzerland	State	Signatory	Purchaced/Used	
United Kingdom	State	Signatory	Purchaced/Used	
United States	State	Signatory	User (Pegasus, Graphite) **Host**	**Paragon Solutions**

"Participant" states and international organisation are outlined in the annex to Pall Mall Declaration.

"Signatory" states are outlined in the annex to Pall Mall Code of Practises.

Authors:

SOLOMIIA VYBRANOVSKA
Expert of the Economic Security Council of Ukraine (ESCU) s.v@escu.ua

DR. ILONA KHMELEVA
Secretary of the Economic Security Council of Ukraine (ESCU) khmeleva@escu.ua

The research was prepared by the Economic Security Council of Ukraine (ESCU)
in cooperation with the Trusted Tech Caucus at the Verkhovna Rada of Ukraine.