Bringing Technology Back into Spyware Regulations

AMIT SHENIAK*

TABLE OF CONTENTS

I. INTRODUCTION

Professor Lubin's "Selling Surveillance" provides insightful information on the current attempts to promote legal solutions to the pressing international challenge of commercial spyware proliferation that has emerged as a critical challenge to human rights, democratic institutions, and national security. [1] Amid recent revelations of the extensive use of sophisticated surveillance tools like Pegasus, Predator, and Hermit against journalists, human rights defenders, politicians, and diplomats worldwide, Lubin's article provides an invaluable critique of the current international efforts to establish regulatory frameworks for the commercial spyware industry, which has long operated in a legal grey zone between legitimate law enforcement tools and dangerous cyber weapons. His article is setting the scene for a policy-oriented academic and applied research, whose framework I will try to set forth, while using his insightful observations as an empirical scaffolding to describe in broad terms how we should move forward with spyware export control.

The evolving landscape of cyber capabilities demands a fundamental shift in how we approach spyware export controls. Current policies often rely on binary decisions—either permitting or prohibiting exports based on simplified criteria—which fails to address the complex reality of these sophisticated tools, and the hard reality that Lubin acknowledges, that the spyware services and products are considered by most governments as legitimate—and therefore are here to stay.[2] This response paper argues for a more nuanced approach that should integrate two critical and often neglected dimensions: comprehensive

* Amit Sheniak is a Senior Research fellow at the Shasha center for Strategic Research and the Cyber Security Research Center (HCSRC), Hebrew University of Jerusalem. His research explores the social and political context and effect on security policy of emerging and disruptive technologies and technological innovation processes.

[1] Asaf Lubin, *Selling Surveillance*, 85 OHIO ST. L.J. 809, 809, 812, 815 (2025).

[2] *See id.* at 812, 814, 816.

technical analysis and spyware-oriented geo-strategic assessment. The technical component would extend beyond basic capability evaluation to encompass the full spectrum of potential applications, vulnerabilities, and collateral impacts of cyber tools. This technical understanding must then be contextualized within a sophisticated political and geo-strategic framework that considers regional power dynamics, governance structures, internal legislation, history of misuse, and potential implications for international relations.

My argument proceeds through several interconnected stages of analysis to present a basic framework for the policy formation of spyware export controls. It begins by examining Professor Lubin's insightful work on cyber export policy, building upon his theoretical and empirical legal foundations while identifying a potential policy impediment, which is the lack of scale to measure spyware export decision-making. The discussion then advances to incorporate critical technical dimensions, demonstrating how detailed technological analysis can broaden the spectrum of policy options available to decision-makers. The core contribution of this work lies in its development of an integrated analytical framework that can serve as a scale for spyware decision-making that synthesizes both technical capabilities and geo-strategic implications of commercial spyware exports. The paper concludes by outlining the broader implications of this dual-analysis approach for future cyber export control policies and identifying promising directions for subsequent research in this rapidly evolving domain.

II. THE NEED FOR SCALE-BASED SPYWARE POLICY FRAMEWORK

The political context of Lubin's analysis highlights its importance, driven by the growing urgency of regulating commercial spyware, a need highlighted by a series of high-profile surveillance incidents that have shaken the international community. These include the targeting of U.S. diplomatic personnel in Uganda, the surveillance of European Commission officials, and the systematic monitoring of civil society actors worldwide.[3] Such incidents that were exposed between 2022 and 2023 prompted unprecedented action from the United States government, culminating in President Biden's Executive Order

[3] Katie Benner, David E. Sanger & Julian E. Barnes, *Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa*, N.Y. TIMES (Dec. 3, 2021), https://www.nytimes.com/2021/12/03/us/politics/phone-hack-nso-group-israel-uganda.html [https://perma.cc/ZU6Q-DMBV]; Raphael Satter & Christopher Bing, *Exclusive: Senior EU Officials Were Targeted with Israeli Spyware*, REUTERS (Apr. 11, 2022), https://reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/ [https://perma.cc/Y5BV-J3B8]; *Global: 'Predator Files' Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials*, AMNESTY INT'L (Oct. 9, 2023), https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/ [https://perma.cc/PXQ5-WP89].

14093.[4] In signing this order, Biden articulated a clear position: "this Executive Order demonstrates the United States' leadership in, and commitment to, advancing technology for democracy, including by countering the misuse of commercial spyware and other surveillance technology . . . to deepen international cooperation to promote responsible use of surveillance technology, counter the proliferation and misuse of such technology, and spur industry reform.."[5]

This decisive statement not only marked a fundamental shift in U.S. policy regarding commercial surveillance technologies but also established a new benchmark for international responses to the spyware threat.[6] Therefore, this Article's necessity is clear given the emergence of multiple, overlapping international initiatives. It does not, however, address or mention a growing number of policy research from academia or leading think tanks that are highlighting the need to generate useful knowledge for relevant public practitioners to be able to advance informed policies. For instance, the U.K.-led Pall Mall Process, which was addressed by Lubin, has been informed by groundbreaking policy research from prominent institutions such as Chatham House's comprehensive report on the global spyware market that has highlighted critical gaps in existing regulatory frameworks,[7] and RUSI's technical analysis of surveillance technologies has provided valuable insights into potential control mechanisms.[8] The Carnegie Endowment for International Peace has also published influential policy recommendations focusing on the intersection of commercial spyware and national security, emphasizing the need for coordinated international responses.[9] These think tanks have played a crucial

---

[4] Exec. Order No. 14,093, 88 Fed. Reg. 18957 (Mar. 30, 2023).

[5] *FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware That Poses Risks to National Security*, THE WHITE HOUSE, (March 27, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/ [https://perma.cc/WMB5-BMHX].

[6] Dorothy Shea, Remarks at a UN Security Council Arria-Formula Meeting on Commercial Spyware (Jan. 14, 2025), https://usun.usmission.gov/remarks-at-a-un-security-council-arria-formula-meeting-on-commercial-spyware/#:~:text=We%20also%20call%20on%20governments,peaceful%20assembly%2C%20and%20protecting%20and [https://perma.cc/8PMT-GS4Z].

[7] *See* JAMES SHIRES, PRINCIPLES FOR STATE APPROACHES TO COMMERCIAL CYBER INTRUSION CAPABILITIES: NAVIGATING THE POLICY CHALLENGES OF CYBER INTRUSION MARKETS 5, 16–17 (2024), https://www.chathamhouse.org/sites/default/files/2024-10/2024-10-18-state-approaches-cyber-intrusion-shires.pdf [https://perma.cc/5JCR-UTCC].

[8] GARETH MOTT, JAMES SHIRES, JEN ELLIS, JAMES SULLIVAN & JAMIE MACCOLL, STATE PERMISSIVE BEHAVIOURS AND COMMERCIAL OFFENSIVE-CYBER PROLIFERATION 30–32 (2024), https://static.rusi.org/permissive-state-behaviours-commercial-offensive-cyber-proliferation-final.pdf [https://perma.cc/Z589-QP5V].

[9] Emma Landi, *Harmonizing Recent Campaigns to Tame the Hacking Marketplace*, CARNEGIE ENDOWMENT FOR INT'L PEACE (June 25, 2024), https://carnegieendowment.org/

role in shaping the policy discourse, providing evidence-based recommendations that bridge technical understanding with policy requirements, and helping to establish a common framework for evaluating the effectiveness of proposed regulatory measures. Yet, they tend to base their analysis on the common purist human-rights approach and might benefit from Lubin's critical description of the status of international actions and legal discourse.

I align with Lubin's balanced approach to commercial spyware regulation, which skillfully navigates between the extremes of human rights absolutism and unfettered national security imperatives to promote constructive dialogue and actionable policy solutions.[10] His framework advocates for a comprehensive global control and accountability regime anchored in human rights standards, emphasizing the importance of engaging corporations and civil society through a multistakeholder approach.[11] Lubin's critique of proposals calling for a global spyware moratorium is particularly incisive; he convincingly argues that such blanket prohibitions are not only impractical but could potentially compromise public safety and the security of information and communication technologies.[12] Furthermore, he sharply identifies a fundamental challenge in achieving accountability: the inherent tension between transparency and the legitimate need to protect sensitive operational details, whether driven by national security considerations or proprietary business interests.[13] This nuanced analysis recognizes that effective regulation must balance competing interests while maintaining meaningful oversight mechanisms.

Thus, Professor Lubin's noteworthy contribution provides a comprehensive analysis of the international, bilateral, multilateral, and national approaches to addressing the regulatory challenges posed by commercial spyware. His article's emphasis on legal frameworks and human rights considerations offers valuable insights into the current regulatory landscape. Through meticulous documentation of both the limitations and potential benefits of international legal regimes, Lubin establishes an essential foundation for understanding contemporary regulatory approaches.[14] He advances beyond traditional legal scholarship by proposing concrete recommendations for government and corporate obligations.[15] However, while these recommendations significantly advance the discourse, they could be further enhanced through the development of more specific policy frameworks for decision-making. His article expertly advances our understanding of the legal landscape but stops short of providing decision-makers with concrete tools for implementation. I argue that the current evolution of the commercial spyware market demands a more granular

research/2024/06/us-europe-cyber-policy-joint-statement-pall-mall-process?lang=en [https://perma.cc/BV2Z-JSTE].

[10] *See* Lubin, *supra* note 1, at 867.

[11] *Id.* at 866.

[12] *Id.* at 814.

[13] *See id.* at 825, 843.

[14] *See, e.g.*, *id.* at 861.

[15] *Id.* at 866–871.

approach—specifically, a systematic scale that decision-makers can employ to evaluate export decisions. Such a scale requires careful translation of the various technological dimensions that constitute spyware tools, enabling more nuanced and effective regulatory choices when cross-examined with a spyware-oriented political and geo-strategic analysis.

Drawing on Sheila Jasanoff's insight about the crucial role of scientific knowledge in shaping regulatory frameworks,[16] this paper argues for the development of a comprehensive technical scale for evaluating commercial spyware exports. Despite the growing discourse around surveillance technology regulation, the existing literature has notably failed to construct a systematic technical framework for assessing these tools' capabilities and risks. Current policy discussions often rely on broad categorizations that fail to capture the nuanced technical distinctions between different surveillance systems. A technically based scaling system would provide policymakers with concrete metrics for evaluation across multiple dimensions: the scope and depth of data collection capabilities, the level of system autonomy, the potential for unauthorized proliferation, integration with existing surveillance infrastructure, and the technical expertise required for responsible deployment. Such granular technical understanding would enable more sophisticated export decisions that move beyond simple binary approvals or denials. This technical scaling approach would empower expert decision-making by providing a standardized framework for assessing the relationship between specific technical capabilities and their potential impact in varying political and social contexts.

III. BRING TECHNOLOGY BACK IN

The absence of detailed technical analysis regarding cyber tools' development processes limits decision makers' abilities to both recommend effective actions and present a realistic view of the spyware market. Historically, the mischaracterization of spyware as similar to limited-collateral radio frequency SIGINT systems has hindered the development of dedicated arms control regulations.[17] A few years ago, these tools were often incorrectly categorized by arms export regulatory regimes as conventional radio-based Signal Intelligence (SIGINT) systems—products that faced fewer restrictions because of their perceived indirect impact on human life, and proved futile for mass surveillance purposes.[18] This claim corresponds with Lubin's critique of

[16] *See generally Expertise and Regulatory Science*, SHEILA JASANOFF, https://sheilajasanoff.org/research/expertise-and-regulatory-science/ [https://perma.cc/SMZ7-5XTY].

[17] See SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS 1 (1976), for an early example that describes spyware as a SIGINT intelligence system used for a passive collection of information.

[18] *See* CORTNEY WEINBAUM, STEVEN BERNER & BRUCE MCCLINTOCK, SIGINT FOR ANYONE: THE GROWING AVAILABILITY OF SIGNALS INTELLIGENCE IN THE PUBLIC DOMAIN 1, 6–8 (2017), https://doi.org/10.7249/PE273 [https://perma.cc/AM9Z-L8MD].

the U.S. Due Diligence obligations standards that fall into the generalization trap of spyware definitions.[19]

As scholars of arms control policies have shown, drawing a parallel with traditional arms control regimes is instructive when addressing the regulations of emerging technologies.[20] Such frameworks succeed not because they attempt the impossible task of eliminating arms trading entirely, but because they establish nuanced guidelines that link technical capabilities with ethical implications. These regimes' strength lies in their ability to create a scale to measure arms export decisions and to differentiate between various weapons systems—tactical versus strategic,[21] conventional versus non-conventional[22]—providing policymakers with a spectrum of options rather than forcing binary choices. This raises crucial questions for spyware regulation: Can we identify degrees of invasiveness in surveillance tools? Is it possible to distinguish between tactical spyware with limited collateral impact and more destructive variants? Are all spyware tools fundamentally equivalent in their capabilities and risks? Most importantly, is an inclusive ban on these tools feasible, or should we pursue more nuanced regulatory approaches?

Understanding the technical architecture of spyware is crucial for developing effective regulatory frameworks, a perspective that resonates with Lawrence Lessig's seminal concept that "code is law."[23] Just as Lessig argued that software code functions as a form of regulation in cyberspace, the technical design choices embedded in spyware systems effectively constitute a form of private lawmaking that shapes surveillance capabilities and limitations.[24] This technological architecture establishes the boundaries of what is possible in digital surveillance, creating what Lessig terms "architectural constraints" that can be as powerful as traditional legal restrictions.[25] Therefore, any meaningful regulatory approach must engage deeply with the technical specifications of spyware systems, recognizing that effective governance requires understanding and potentially influencing these architectural constraints through policy intervention.

---

[19] Lubin, *supra* note 1, at 827–29.

[20] *See* Jane Vaynman, *Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control*, 4 TEX. NAT'L SEC. REV. 34, 35–38 (2021); Erin D. Dumbacher, *Limiting Cyberwarfare: Applying Arms-Control Models to an Emerging Technology*, 25 NONPROLIFERATION REV. 203, 205–6 (2018); Mischa Hansel et al., *Taming Cyber Warfare: Lessons from Preventive Arms Control*, 3 J. CYBER POL'Y 44, 50 (2018).

[21] *See, e.g.*, Hans Kristensen & Robert Norris, *Nonstrategic Nuclear Weapons*, 68 BULL. OF THE ATOMIC SCIENTISTS 96, 97 (2012) (discussing the attempts to define nonstrategic nuclear weapons).

[22] See Benjamin B. Hatch, *Defining a Class of Cyber Weapons as WMD: An Examination of the Merits*, 11 J. STRATEGIC SEC. 43, 45 (2018), for an early attempt to define some cyber tools as WMD.

[23] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) [hereinafter LESSIG, CODE AND OTHER LAWS]; LAWRENCE LESSIG, CODEVERSION 2.0 5 (2006).

[24] LESSIG, CODE AND OTHER LAWS, *supra* note 23, at 86.

[25] *Id.* at 236.

A more sophisticated understanding of technological capabilities could enhance arms-control decision-making while simultaneously fostering greater accountability among software architects, vulnerability researchers, and computer engineers involved in spyware development and sales. These technical experts possess the capability to design surveillance tools according to specific technological constraints and specifications when governments and international institutions establish clear parameters.[26] Furthermore, this technical precision enables the development of standardized definitions for legitimate spyware tools—ones that can be deployed by law enforcement agencies with appropriate safeguards and limitations. By anchoring export controls in concrete technical specifications, we create a framework that not only guides decision-makers but also provides clear engineering parameters for the development of surveillance technologies that balance security requirements with privacy protections and human rights considerations.

Jasanoff's concepts of co-production and constitutionalism provide additional theoretical grounding for this technology-aware regulatory approach. Through the lens of co-production, we can understand how spyware technologies and their regulation are mutually constitutive—technical capabilities shape regulatory possibilities, while regulatory frameworks influence technological development.[27] This dynamic relationship exemplifies what Jasanoff terms "constitutional moments," where technical systems and governance frameworks evolve together to create new forms of social and political order.[28] In the context of spyware regulation, this theoretical framework suggests that effective policy solutions must emerge from a deep understanding of both technical possibilities and social implications, recognizing that technology and regulation are inextricably intertwined in shaping surveillance practices and their governance.

While legal scholarship, exemplified by Lubin's excellent scholarly work, succeeds in framing the ethical and regulatory challenges of spyware as clear moral dilemmas, the field now requires a more nuanced technical analysis. As indicated by Lubin's critique of the Wassenaar Agreement's attempt to address spyware dual-use, "there remains significant divergence and lack of consistency in the ways export controls for commercial spyware are adopted, implemented, and enforced around the world."[29] Therefore, to effectively regulate the complex realities of the surveillance technology market, I argue we need to develop a more sophisticated taxonomy of spyware tools and their capabilities.

---

[26] See Jon Postel, *Domain Name System Structure and Delegation*, INTERNET ENGINEERING TASK FORCE: REQUEST FOR COMMENTS (March 1994), at 1, 6–7.

[27] *See generally* SHEILA JASANOFF ET AL., STATES OF KNOWLEDGE: THE CO-PRODUCTION OF SCIENCE AND THE SOCIAL ORDER (2004).

[28] Sheila Jasanoff, *Constitutional Moments in Governing Science and Technology*, 17 SCI. ENG'G ETHICS 621, 623–24 (2011). ("[C]onstitutional moments may encompass the relationship between experts, who underwrites almost all contemporary state action, and citizens, who are collectively subject to the decisions of states.").

[29] Lubin, *supra* note 1, at 820.

This technical understanding would enable policymakers to make more precise distinctions between different categories of surveillance technologies—differentiating between tools that, while problematic, might serve legitimate law enforcement purposes, and those whose capabilities are so intrusive that they should be categorically prohibited. Such technical granularity would provide decision-makers with a more refined framework for evaluating and regulating these technologies, moving beyond binary prohibitions toward more calibrated regulatory approaches that reflect the complex technical and ethical landscape of modern surveillance tools.

Therefore, my attempt to continue Professor Lubin's play and "to score with the ball" he has situated so adequately in front of the opponent's net, is by advocating for reintegrating technological considerations crossed with geostrategic analysis into spyware regulation frameworks. This approach, which might be termed under the framework of "policy-by-design," recognizes that technical challenges often require technically-informed solutions. Governments are increasingly adopting this perspective, incorporating technical specifications and standards into their regulatory frameworks.[30] This trend is evident in emerging bilateral and multilateral initiatives, where technical standards and specifications are becoming integral components of international cooperation efforts.[31] Rather than treating spyware regulation as purely a legal or policy challenge, this approach acknowledges that effective oversight must be built upon a deep understanding of the underlying technology, enabling the development of more precise, targeted, and implementable regulatory measures.

The concept of policy-by-design represents a paradigm shift in regulatory thinking.[32] This approach integrates technical controls and safeguards directly into the policy framework, similar to how privacy-by-design principles have transformed data protection regulations.[33] For instance, mandatory implementation of technical measures such as code signing, secure boot processes, and runtime integrity checking can create substantial barriers to spyware deployment.[34] These technical requirements, when embedded in

---

[30] *See generally* DAN BREZNITZ & MICHAEL MURPHREE, U.S.–CHINA ECON. & SEC. REV. COMM'N, THE RISE OF CHINA IN TECHNOLOGY STANDARDS: NEW NORMS IN OLD INSTITUTIONS (2013).

[31] *See generally* SCOTT ROSE ET AL., NATIONAL INST. OF STANDARDS & TECH., ZERO TRUST ARCHITECTURE (2020) (describing the zero-trust cybersecurity standard).

[32] CHRISTIAN BASON ET AL., DESIGN FOR POLICY 2 (Christian Bason & Rachel Cooper eds., 2016).

[33] Seda Gurses et al., *Engineering Privacy by Design*, INT'L CONF. ON PRIV. & DATA PROT. (2011), https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf [https://perma.cc/CYE9-PX4P]; Peter Schaar, *Privacy by Design*, 3 IDENTITY IN THE INFO. SOC'Y 264, 271 (2010); Kjetil Rommetveit & Niels van Dijk, *Privacy Engineering and the Techno-Regulatory Imaginary*, 52 SOC. STUD. OF SCI. 853, 855 (2022).

[34] *See, e.g.*, *Code Integrity with Secure Boot*, BLUE GOAT CYBER, https://bluegoatcyber.com/blog/code-integrity-with-secure-boot/#:~:text=This%20mechanism%20ensures%20that%20only,gatekeeper%2C%20safegusafegu%20the%20system's%20integrity [https://perma.cc/S6DJ-F59L].

regulatory frameworks, create proactive protection rather than reactive enforcement. Another key advantage of technical solutions in spyware regulation is their ability to provide immediate and automated enforcement. While traditional regulatory measures often rely on detection, reporting, and legal action—processes that can take months or years—technical controls can prevent or impede spyware deployment in real-time.[35] For example, mandatory application sandboxing, implemented through technical specifications in regulatory requirements, can automatically restrict software's ability to access sensitive system resources without explicit user consent.[36]

This policy-by-design approach is already manifesting in various international efforts. For instance, both the U.K.-led Pall Mall Process and recent U.S. initiatives that were analyzed in Lubin's article incorporate specific technical requirements and standards into their regulatory frameworks.[37] These efforts demonstrate a growing recognition that effective spyware regulation must bridge the gap between technical capabilities and policy objectives, creating mechanisms that are both technically feasible and policy-effective. Other recent examples that demonstrate the potential of technical solutions in spyware regulation are the European Union's proposal for mandatory security updates and vulnerability disclosure requirements, which represent a technical approach to reducing spyware attacks.[38] Similarly, Apple's implementation of app tracking transparency features,[39] while not specifically targeting spyware, shows how technical controls can be effectively mandated through policy to enhance privacy protection.

IV. UNPACKING THE COMMERCIAL SPYWARE BLACK BOX: A TECHNICAL TAXONOMY FOR SPYWARE

Professor Lubin was right again to point out that the "NSO Group has been the favored punching bag of human rights activists and privacy advocates, it is by no means the only company on the market."[40] Furthermore, I will add that while the NSO group's Pegasus platform has become the paradigmatic example of commercial spyware in academic literature and policy discussions warning

---

[35] *See, e.g.*, HENG YIN & DAWN SONG, DYNAMIC SPYWARE ANALYSIS (USENIX Annual Technical Conference, 2007).

[36] *See generally* ARTO NIEMI, SURVEY OF REAL-WORLD PROCESS SANDBOXING (35th Conference of the Fruct Ass'n, 2024).

[37] *See* THE PALL MALL PROCESS: TACKLING THE PROLIFERATION AND IRRESPONSIBLE USE OF COMMERCIAL CYBER INTRUSION CAPABILITIES, 2 (2024), https://assets.publishing.service.gov.uk/media/65c25bb23f6aea0013c1551a/The_Pall_Mall_Process_tackling_the_proliferation_and_irresponsible_use_of_commercial_cyber_intrusion_capabilities.pdf?ref=news.risky.biz [https://perma.cc/MJQ5-S7HQ]; Lubin *supra* note 1, at 840, 863.

[38] *See generally* Cyber Resilience Act 2024, 2024 O.J. (L 2024/2847).

[39] *App Tracking Transparency*, APPLE DEVELOPER DOCUMENTATION, https://developer.apple.com/documentation/apptrackingtransparency [https://perma.cc/F9LT-MFTD].

[40] Lubin, *supra* note 1, at 811.

of its "Zero-Click" capabilities,[41] this focus increasingly obscures the profound transformation occurring within the surveillance technology market. The contemporary landscape of offensive cyber capabilities has evolved beyond traditional, integrated spyware platforms toward more sophisticated and fragmented offerings that present novel regulatory challenges.[42] This shift is characterized by the emergence of specialized markets for isolated technical vulnerabilities, modular exploitation frameworks, and cloud-based surveillance infrastructure.[43] Companies now often sell discrete components—such as zero-day exploits, code execution modules, or data extraction capabilities—rather than complete surveillance solutions.[44] This fragmentation of the spyware supply chain makes traditional regulatory approaches, which were conceived with monolithic platforms like Pegasus in mind, increasingly obsolete.[45] Moreover, the rise of "surveillance-as-a-service" models, where capabilities are provided through cloud infrastructure or commercial data brokers, fundamentally challenges conventional notions of export controls and end-user contract or licensing restrictions.[46] This evolution demands a reconceptualization of regulatory frameworks to address not just the end products but the entire ecosystem of surveillance capabilities and services that constitute the modern offensive cyber market. In other words, we need to unpack the technical structure of different spyware tools and services.

Opening the "black box" of spyware's technical architecture is essential for addressing two critical regulatory challenges in contemporary surveillance technology governance. First, the inability to distinguish between different capabilities and deployment methods has led to oversimplified, binary regulatory approaches that overlook the nuanced spectrum of surveillance technologies, treating them uniformly as negative cyber-related tools and services.[47] Understanding the engineered structure of these tools—from their exploitation mechanisms and attack vectors to their data collection architectures—could enable policymakers to develop scaled regulatory

---

[41] *Id.*

[42] Alexandra Paulus & Sven Herpig, *The Pall Mall Process on Cyber Intrusion Capabilities*, LAWFARE BLOG, (Mar. 19, 2024), https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities [https://perma.cc/P3TU-NFSD].

[43] *See* M. Anwar Hossain, *Framework for a Cloud-Based Multimedia Surveillance System*, 10 INT'L J. OF DISTRIBUTED SENSOR NETWORKS 135257, 135258 (2014) (discussing cloud-based surveillance); *see* Bruce Schneier, *The NSA Is Hoarding Vulnerabilities*, SCHNEIER ON SECURITY (Aug. 26, 2016), https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html [https://perma.cc/5N8B-H38X] (discussing vulnerability hoarding).

[44] *See Demystifying the Market for Zero-Day Software Exploits*, PACKETLABS, https://www.packetlabs.net/posts/demystifying-the-market-for-zero-day-software-exploits/ [https://perma.cc/46T7-HQ6A].

[45] *See* Lubin *supra* note 1, at 811.

[46] *See generally* YUNG AU, SURVEILLANCE AS A SERVICE: THE EUROPEAN AI-ASSISTED MASS SURVEILLANCE MARKETPLACE (Oxford Comm'n on AI & Good Governance 2021).

[47] *See, e.g.*, THE PALL MALL PROCESS, *supra* note 37, at 6 (expanding the spyware definition to include "Hacker for Hire" services), and Paulus & Herpig, *supra* note 42.

responses similar to those employed in conventional arms control regimes. Second, the rapid evolution of the commercial spyware market, particularly the emergence of disaggregated business models such as the isolated sale of "zero-day" vulnerabilities (referred to by Lubin as "vulnerabilities hoarding"), and the exploitation of digital advertising infrastructure for surveillance purposes (also known as "malvertising"), demands regulatory frameworks that engage with specific technical components rather the existing mechanisms that are geared toward regulating companies that manage complete systems and service that might be easier to monitor.[48] This granular technical understanding would enable regulators to address not just traditional, monolithic spyware platforms but also the growing marketplace for surveillance capabilities delivered through component services, cloud infrastructure, and commercial data brokers. By unpacking and classifying the technical architecture of these systems, policymakers can develop more adaptive and effective regulatory frameworks that address both current and emerging surveillance technologies while maintaining the flexibility to respond to future technological innovations. As the NSO case can teach us, improving the regulatory framework will demand a combination of these technical taxonomies and political assessment.

The development of a nuanced taxonomy for cyber-surveillance tools, distinguishing between what I coin as "tactical vs. strategic" spyware capabilities, is essential for effective regulation that necessitates a concrete instrumental scale to be able to develop a more accurate and nuanced policy. This classification can be structured around several key technical parameters. First, the scope of targeting capabilities, where tactical tools might be limited to specific devices or networks, while strategic platforms can penetrate multiple layers of digital infrastructure simultaneously.[49] Second, physical proximity requirements, where tactical tools often necessitate close-range deployment or local network access, contrast with strategic platforms that can operate across global networks without geographical constraints (also known as "Remote Delivery Vector").[50] Third, the defendability factor, where tactical tools typically exploit known vulnerabilities that can be patched or mitigated through standard cybersecurity measures, whereas strategic platforms often leverage zero-day exploits or sophisticated and unknown attack vectors that are

---

[48] *See* Xinyu Xing et al., *Understanding Malvertising Through Ad-Injecting Browser Extensions*, 2015 PROCEEDINGS OF THE 24TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB, WWW '15 1286 (Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2015); Lubin, *supra* note 1, at 834.

[49] See Lubin, *supra* note 1, at 811, for an example of a spyware platform with multi-layer penetration capabilities, consider NSO's Pegasus, which relies on a series of undiscovered software vulnerabilities, known as "zero-day exploits," to infiltrate devices.

[50] See ERIC CHIEN, TECHNIQUES OF ADWARE AND SPYWARE 8 (2005), https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ed66158a0a8818ed20df f303354264dc4cb5c06a [https://perma.cc/8BNW-TPJP] for an explanation about the different types of cyber tool delivery "vectors."

significantly harder to detect and prevent.[51] Fourth, the scale of simultaneous deployment, where tactical tools are generally limited in their concurrent targeting capabilities, while strategic platforms can conduct mass surveillance across thousands of targets simultaneously.[52] Finally, the analytical capabilities, where tactical tools usually focus on specific data extraction, while strategic platforms incorporate advanced algorithms and artificial intelligence to process vast amounts of intercepted data into actionable intelligence.[53] These distinctions are crucial for developing graduated regulatory responses that recognize the varying degrees of risk and potential harm associated with different categories of surveillance technologies.

V. CROSSING TECHNOLOGY WITH GEOSTRATEGIC ASSESSMENT

The proliferation of commercial spyware technologies has created an urgent need for sophisticated geo-strategic and political analysis frameworks to inform export control policies. While traditional export control regimes focus primarily on general technical capabilities classification and end-use verification, the unique characteristics of surveillance technologies demand a more nuanced approach that considers complex political dynamics, human rights implications, and regional power balances. A comprehensive analytical framework must evaluate not only the immediate security implications of spyware exports but also assess how these technologies might alter domestic political landscapes, affect regional stability, or enable the suppression of civil society in recipient nations. Furthermore, the dual-use nature of many surveillance technologies, combined with the rapid pace of technological advancement, requires regular reassessment of how these tools might be weaponized against democratic institutions or exploited by authoritarian regimes. This necessitates the development of dedicated analytical capabilities that can synthesize intelligence on political trends, human rights conditions, and internal national technological regulations and legislation, to form coherent and adaptable export policies that protect both national security interests and democratic values. As a point of embarkment for this kind of analytical framework, I suggest the following criteria: (1) governance structures and political stability, (2) internal and

---

[51] *See* LILLIAN ABLON & ANDY BOGART, ZERO DAYS, THOUSANDS OF NIGHTS: THE LIFE AND TIMES OF ZERO-DAY VULNERABILITIES AND THEIR EXPLOITS 2–3 (2017).

[52] *See generally* Ronald J. Deibert, *The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy*, FOREIGN AFFS. (Dec. 12, 2023), https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert (discussing mass surveillance).

[53] *See* Brant C. Reilly, *Doing More with More: The Efficacy of Big Data in the Intelligence Community*, 32 AM. INTEL. J. 1, 21 (2015). S*ee generally* Rongjunchen Zhang et al., *Using AI to Attack VA: A Stealthy Spyware Against Voice Assistances in Smart Phones*, 7 IEEE ACCESS: SPECIAL SECTION ON SEC. & PRIV. IN EMERGING DECENTRALIZED COMMC'N ENV'TS 153542 (2019) (discussing the convergence between AI and spyware).

institutional power dynamics, (3) relevant national legislation and regulations, and (4) potential implications for international and regional relations.

One of the main arguments presented by spyware companies is that they sell their product to official and legitimate government agencies to allow them to fight incurable national threats such as terrorism and organized crime organizations.[54] Thus, the governance structures of potential recipient nations are a crucial dimension in evaluating spyware exports. The institutional framework within which surveillance technologies will be deployed directly impacts their potential for misuse or abuse. Countries with robust oversight mechanisms, independent judiciary systems, and strong privacy protections are better positioned to ensure the responsible deployment of these tools. Conversely, nations lacking transparent governance structures or with a history of surveillance abuse, whether by the aid of cyber tools or not, pose heightened risks. The analysis must extend beyond formal institutional arrangements to consider informal power structures, the relationship between security services and political leadership, and the effectiveness of civilian oversight mechanisms. Understanding these governance dynamics is essential for developing export policies that can differentiate between responsible and problematic end-users while accounting for the varying levels of institutional maturity across different political systems.

The internal national power dynamics of potential recipient countries represent a critical criterion for evaluating commercial spyware exports. The relationship between government institutions, civil society organizations, and media outlets provides a crucial context for assessing how surveillance technologies might affect democratic processes and civil liberties. In countries where power is heavily concentrated within security agencies or where there is limited oversight of law enforcement operations, advanced spyware capabilities could further erode checks and balances. Additionally, the competition and coordination between different law enforcement and intelligence agencies must be considered, as inter-agency rivalries or lack of coordination could lead to uncontrolled proliferation of surveillance capabilities within the state apparatus. The relative strength of independent media and civil society organizations serves as a particularly important indicator, as these institutions often provide essential oversight and public accountability for the use of surveillance technologies.[55] The outcome of such analysis can also lead to differentiated policy toward different government entities in the same county (i.e., between federal or national agencies to local or state-level authorities).

The national legal framework surrounding digital rights and state surveillance powers provides another essential criterion for assessment.

---

[54] *See, e.g.*, *NSO Group - About Us*, NSO GRP. TECHS., https://www.nsogroup.com/about-us/ [https://perma.cc/R6XV-E7EX].

[55] *See* IAN DAVIS, BUILDING INTEGRITY AND REDUCING CORRUPTION IN DEFENCE: A COMPENDIUM OF BEST PRACTICES 261–80 (2010), https://gsdrc.org/document-library/the-role-of-civil-society-and-the-media/ [https://perma.cc/4QKH-KH25].

Countries vary significantly in their legislative approaches to cybersecurity, privacy protections, and governmental surveillance authorities.[56] The existence and enforcement of data protection laws, requirements for judicial oversight of surveillance activities, and legal limits on government intrusion into private communications all indicate the potential for responsible use of spyware technologies. Historical patterns of internet shutdowns, content filtering, and digital surveillance can reveal how new surveillance capabilities might be deployed within existing legal structures.[57] Furthermore, the transparency of surveillance warrants processes and the ability of citizens to challenge surveillance operations through legal channels should significantly influence export policy decisions. At the more general level, it boils down to the different national perceptions of the elusive concept of digital or cyber sovereignty, an issue that has far more practical and implemental ramifications than the way we usually think about it, and that demands extensive research.

Political stability and the potential impact of surveillance technologies on civil unrest present a third crucial criterion for evaluation. In politically volatile environments, commercial spyware could be weaponized to suppress legitimate political dissent and peaceful demonstrations. The historical pattern of how semi-democratic or authoritative regimes and governments respond to civil unrest, their treatment of political opponents, and their approach to managing public protests should inform export decisions.[58] Moreover, in countries experiencing political transitions or facing significant social tensions, the introduction of advanced surveillance capabilities could dramatically alter the balance of power between state security forces and civil society movements or foster the erosion of democratic changes of power. The potential for these technologies to be used in targeting protest organizers, tracking political opponents, or conducting mass surveillance during periods of civil unrest must be carefully weighed against legitimate law enforcement needs.

The regional power dynamics surrounding commercial spyware exports are another political criterion that warrants careful consideration, as these technologies can significantly alter the balance of power between neighboring states. When advanced surveillance capabilities are introduced into regions with existing tensions or power asymmetries, they can exacerbate instabilities and trigger security dilemmas.[59] For instance, if one state in a contested region acquires sophisticated spyware capabilities, its neighbors may feel compelled to

---

[56] *See generally* SANJA KELLY, MAI TRUONG, ADRIAN SHAHBAZ, MADELINE EARP & JESSICA WHITE, FREEDOM HOUSE, FREEDOM ON THE NET 2017, at 45 (2017), https://freedomhouse.org/sites/default/files/2020-02/Freedom_on_the_Net_2017_complete_book.pdf [https://perma.cc/6QUP-8RDJ].

[57] *See* Nurul Momen, Harsha S. & Debobrata Das, *Mediated Democracy and Internet Shutdown in India*, 19 J. INFO., COMMC'N & ETHICS SOC'Y 2, 2–5 (2020) (India can be considered as a potential example).

[58] *See* KELLY, *supra* note 56.

[59] BEN BUCHANAN, THE CYBERSECURITY DILEMMA: HACKING, TRUST AND FEAR BETWEEN NATIONS 1–3 (2017).

pursue similar technologies, potentially initiating an arms race in the cyber domain. Moreover, regional hegemons might leverage their access to advanced surveillance technologies to extend their influence over smaller states, while simultaneously using these tools to monitor potential challenges to their authority from within the region. This complex interplay between cyber capabilities and regional power structures necessitates a nuanced export policy that considers not only bilateral relations but also broader regional stability implications. Additionally, some cases should be translated to specific demands by the regulator to technically limit spyware use to the state's sovereign territory.

The international relations implications of commercial spyware exports extend far beyond immediate bilateral relationships, potentially affecting global diplomatic dynamics and international norm development. The transfer of sophisticated surveillance technologies can serve as a tool of diplomatic leverage, creating new dependencies and allegiances between states. Furthermore, the proliferation of these capabilities can influence international cooperation on cybersecurity, privacy standards, and human rights protection. There are also significant reputational risks for exporting nations, as their decisions regarding spyware exports may affect their standing in international forums and their relationships with other states. The growing global debate over digital sovereignty and cyber governance adds another layer of complexity, as decisions about spyware exports increasingly intersect with broader discussions about technological independence, data protection, and the future of international cyber norms.[60]

VI. SUMMARY

Lubin's goal to provide a pragmatic account of the installation of an international spyware regulatory framework should be praised. His advocacy for a pragmatic and centrist approach that "seeks to foster a nuanced dialogue that recognizes the intricacies of modern intelligence operations" indeed reflects a "commitment to constructive engagement, dialogue, and practical policymaking in an increasingly polarized world."[61] The question remains whether one can accomplish these goals without delving into the technology itself, its challenges, and promises. How otherwise could both policymakers and scholars not avoid the need to create a normative framework that could provide legitimacy to the places where the use of spyware is needed to confront current security challenges?

---

[60] *See* Letter from Burhan Gafoor to United Nations (July 11, 2024), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_11_July_2024.pdf [https://perma.cc/7Y67-6ATY].

[61] Lubin, *supra* note 1, at 874.

This Article builds upon Lubin's foundational work by translating his legal scholarship into a practical framework that incorporates science, technology, society perspectives, and practitioner insights. The proposed approach combines a nuanced technical taxonomy of spyware tools with targeted political and geostrategic analysis of potential recipients, whether state or non-state actors. This synthesis of technical and political assessment provides national and multilateral institutions with an instrumental framework for developing more sophisticated export control mechanisms—ones that transcend binary approval decisions. Such an approach enables precise risk assessment while accommodating conditional approvals, tiered access, and dynamic oversight mechanisms, better serving both security interests and commercial realities in our rapidly evolving cyber landscape. Given the global nature of spyware proliferation,[62] international coordination in technical standards and regulatory approaches becomes crucial. Technical specifications embedded within policy frameworks must be harmonized across jurisdictions to prevent the emergence of security havens where weaker requirements could be exploited. In this context, international standards organizations could play a vital role in developing and maintaining technical specifications that align with and support broader regulatory objectives.

In conclusion, Professor Lubin's scholarly work not only emphasizes the need for pragmatic international legal solutions but also provides a foundation for policy experts and cyber practitioners to develop more sophisticated frameworks for spyware export decisions. While technical specifications alone cannot fully address the challenges posed by commercial spyware, their integration with dedicated political analysis creates opportunities for more effective regulation. The policy-by-design approach, which incorporates technical requirements as fundamental elements of regulatory frameworks, offers a promising direction for future development. Moving forward, successful spyware regulation will depend on sustained collaboration between technical experts, legal scholars, policymakers, and industry stakeholders to create and implement comprehensive frameworks that balance security needs with human rights protections. Such frameworks must bridge the gap between abstract legal principles and concrete technical specifications, enabling more nuanced and effective export control decisions in an increasingly complex digital landscape.

---

[62] *See* Jen Roberts et al., *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*, ATL. COUNCIL, (Sept. 4, 2024), 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/#:~:text=Despite%20its%20contribution%20to%20human,only%20a%20handful%20of%20vendors [https://perma.cc/4YN2-3UZK].