Atlantic Council
CYBER STATECRAFT INITIATIVE

March 2026

# Issue brief

# Mythical Beasts: Investigating the role of intermediaries in the proliferation of offensive cyber capabilities

Written by Jen Roberts, Sarah Graham, and Lyla Renwick-Archibold

***Mythical Beasts is an ongoing project by the Atlantic Council's Cyber Statecraft Initiative documenting the proliferation of offensive cyber capabilities like spyware. The 'mythical beasts' here refers to the common practice of vendors in the spyware market taking names from fantasy and mythology for their products.***

## Executive Summary

The marketplace for offensive cyber capabilities (OCCs) has become increasingly complex over time. Contributing to this complexity are intermediaries—entities that serve a critical yet poorly understood role in the proliferation of this industry. Largely due to the private nature of intermediary relationships and transactions, there is limited public knowledge about these intermediary entities that bridge relationships and transfer goods within the OCC supply chain.

As governments and international processes seek to establish norms and regulations for this highly fragmented OCC industry through initiatives including the ongoing multistakeholder Pall Mall Process, the lack of shared public knowledge is a significant hurdle. The opacity of this market subsection poses policy challenges and complicates efforts to regulate these entities. This undermines transparency, accountability, compliance, and due diligence, and threatens to enable the unchecked proliferation of these capabilities to end users who abuse them.

This research draws on expert roundtable interviews and vignettes that shine light on intermediary functions and their effects on the wider market—features of the supply chain that still confound researchers and policymakers alike. Building on research in the Mythical Beasts project series, this issue brief maps intermediary roles and effects, with an aim to enable more precise, effective policies to curb abusive proliferation while maintaining the legitimate security research and defensive capabilities that these entities can offer.

## Introduction

As technological and regulatory evolutions in offensive cyber capabilities (OCCs) continue, the landscape of tools, vulnerabilities, and skills leveraged for sophisticated and targeted operations continues to adapt. However, many states turn to the open market to procure these often highly specialized products and services, due in part to limited in-house capacity among other factors. In recent years, the marketplace for these OCC products and services has continued to evolve and proliferate—as evidenced in the Atlantic Council study on the global spyware market, Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and its Threats to National Security and Human Rights. This research and other global mapping initiatives shed light on the complex supply chains of OCCs, a complexity and opacity that pose challenges to meaningful marketplace transparency and accountability.

A key feature of the marketplace—intermediaries, which are entities that provide essential products or services that support a final OCC product—continues to be largely fragmented, with minimal shared public knowledge on the characteristics, influences, and norms on of the entities operating within the OCC supply chain. As surveyed in the Mythical Beasts project, open-source information about what roles intermediaries play in proliferation and the effects they have on marketplace dynamics is limited, despite academic research and public reporting indicating that there is a heavy reliance on commercial intermediaries.

Intermediaries are fundamentally different than other entities that operate within the marketplace for OCC. Intermediaries are largely found as partners within the OCC supply chain, complimenting product development through vulnerability research to complete exploit chains or as auxiliary support during technology deployment. Unlike OCC vendors, intermediaries are typically not the public face of products; rather, they are better known within private client bases. Intermediaries can be a one-person shop, relying on personal relationships to establish a client network. They can drive up business by facilitating new relationships to previously inaccessible or new customer bases and to increase profits for both themselves and on behalf of vendors that employ them. Altogether, these factors make it more difficult to track and understand the types of relationships and effects that intermediaries have on the OCC market, as limited public information exists about them outside of hacked and leaked documents, investigative reporting, and sporadic transparency initiatives.

As an important aside, the concept of an intermediary can be applied not only to private sector entities but also to states. Third-country intermediaries typically operate in permissive trade environments that act as favorable "stepping stone" jurisdictions; for example, they may offer legal or logistical support that facilitates the movement of spyware and exploits across regulatory boundaries. These jurisdictions themselves operate as an intermediary state hub that is hosting intermediary companies locally domiciled to provide services such as the transfer or export of goods onward to a third country. Although the permissive or restrictive nature of states is a feature of the OCC supply chain, the design of policy interventions for state exports differs from those applied to intermediary entities and, thus, is beyond the scope of this issue brief.

These questions surrounding the characteristics and effects of intermediaries persist not only as they pertain to spyware, but also in how they interact with other components of the OCC supply chain— from the foundation from which they are built, such as vulnerability and exploit research, to the services like training or educational materials they might provide. With the Mythical Beasts project as a jumping-off point, this piece explores intermediary relationships, products, and their effects on submarkets within the larger OCC supply chain for high-end cyber intrusion products. These products, often referred to as spyware, range from software and tools that enable remote access to a computer system without the consent of the user, administrator, or owner of the computer system. With system access, intermediaries are able to collect, exploit, extract, intercept, retrieve, alter, delete, or transmit content.

The limited and siloed knowledge regarding intermediaries creates a significant policy hurdle— these entities contribute to the opaque proliferation of the OCC industry. But how can policymakers enact effective regulation and standards to curb the abusive effects of vendors when they do not understand the perimeters within which these entities operate? This issue brief explores the characterization of intermediaries, the difference between different intermediary types (i.e., broker, reseller), how different intermediaries carry varying effects on the market (i.e., price increases, supply chain muddling) and concludes with policy recommendations to mitigate the effects of these issues, specifically for the ongoing Pall Mall Process.

## Methods

To investigate intermediaries in the OCC marketplace and product supply chain, this brief combines expert interviews with desk review to present a rich description of the characteristics, influences, and norms of intermediaries. The interviews were conducted in fall 2025 in a roundtable format with subject matter experts on the cyber capabilities ecosystem from across the national security and private sectors as well as in one-on-one conversations. Individual interviews were conducted with sources from private sector firms who have interfaced with or researched intermediaries or can be identified as intermediaries themselves (e.g., exploit brokers). For privacy considerations, interviewees remain anonymous but represent the following profiles:

- leaders and senior employees of offensive hacking or vulnerability research companies in the United States or Europe,
- security researchers with expertise in offensive hacking and regional specialties both within and outside the United States, and
- individuals acting as intermediaries that have facilitated relationships and access from individuals or companies to buyer countries based in Five Eyes countries and Europe.

Individual interviews will be cited based on the roundtable that interviewees participated in (e.g., Roundtable #1) to avoid attribution. Due to the lack of public information on intermediaries, interviews are a significant source of descriptive data for this brief. Prior to the roundtables, the authors reviewed academic, policy, and recent media reporting to identify the terms used to refer to entities intermediate to the OCC supply chain. Below, the authors map these terms and seek to clarify the terminology.

## Characterizing the complicated: Defining intermediaries

Cyber intrusion products like spyware are characterized by their sophisticated infection chains, meaning they can combine vulnerabilities and exploits to achieve greater levels of compromise. They are also often valued for their stealth on a target device. A maturing marketplace has emerged to enable the development, sale, and deployment of these products, with intermediaries playing a crucial role in ensuring robust and effective exploit chains and in deploying products with varying degrees of anonymity. Notably, as France's national cybersecurity agency (ANNSI) explains, an intrusion product typically exploits several vulnerabilities as an exploit chain to bypass each application layer and deploy the desired surveillance as close as possible to the system's core. Given this interrelated set of permissions or access points at both a technical and organizational level, there are numerous opportunities for intermediaries to supply products or services.

Across industry materials, policy documents, and technical reporting, a range of terms are used to describe intermediary entities that operate at various junctures in the OCC supply chain. Intermediaries are entities that provide essential products or services that support a final OCC product. For example, they can facilitate access to or transfer of goods (e.g., vulnerabilities) or services (e.g., access-as-a-service) between two or more parties. In different literatures, intermediaries encompass a variety of relationships, including brokers, resellers, contractors, partners, middlemen, infrastructure providers, and even countries as third-party intermediaries. Some of these terms share overlapping responsibilities, while others are distinct. **Here, these terms will be addressed and categorized.**

**Brokers,** sometimes referred to as vulnerability brokers, broker firms, or middlemen, will purchase vulnerabilities or exploit components from researchers and sell them to governments or other clients. Brokers establish their clientele based on relationships with sellers and buyers, and for each transaction, there can be an individual or a chain of brokers that sell said good or service onward to a buyer.[1] Thus, brokers can serve as direct links between the seller and a buyer or can sell to another broker in the chain who then sells to an end client or another broker. Oftentimes, brokers sell a single component of an OCC, rather than a bundled product (i.e., selling an exploit versus selling an OCC product containing an exploit bundled with malware). For instance, Operation Zero, a Russian vulnerability brokerage firm, specializes in acquiring and selling zero-day exploits.

**Resellers,** on the other hand, typically procure and then repackage or rebrand cyber intrusion products to new customers. Crucially, a reseller obtains the rights to a software product and may even modify the product before selling it onward to a new buyer. In practice, repackaging or rebranding means bundling spyware or exploit capabilities with services including technical support, training, and adapting products to local contexts, thus making exploits easier for clients to deploy.[2] Oftentimes, and distinguishable from brokers, resellers bundle products together, reselling a package of products rather than a single component of OCC. Resellers may also lease sup-

1. Roundtable #1 (virtual), November 13, 2025.
2. Roundtable #1.

porting infrastructure to multiple vendors, such as virtual private networks (VPNs) or domain hosting. Frequently, resellers operate within jurisdictions that have favorable or limited regulations, thereby enabling sales across borders.[3] An example of a reseller is RCS Lab, which sold Hermit spyware (Hacking Team/Memento Labs spyware) on behalf of Hacking Team.[4]

Notably, brokers and resellers can operate both "in-house" or as "contractors" for the entity they broker or resell the products for. In-house intermediaries are entities that are owned by an OCC vendor, or other entity in the supply chain. For example, a spyware vendor can own a reseller whose purpose is to resell its spyware to specific countries. Alternatively, vendors can contract a broker or reseller to procure a specific capability, product, or service, or facilitate the sale of a specific capability, product, or service. Below, the authors do not distinguish between in-house and contracted brokers or resellers as it cannot be determined whether they have varying degrees of effect on driving or narrowing proliferation in distinct ways.

**Other terms** in the literature **combine brokers and resellers into one category.** For example, in the defense and intelligence communities, "contractors" serves as a stand-in term for resellers and brokers, used also with "prime contractors" for large system integrators and "subcontractors" for boutique firms or individual researchers.

**Partner** is another term that combines the functions of brokers and resellers with the specific context of the offensive cyber capability of spyware. "Partner" is a term observed in industry materials and used in the Atlantic Council's Mythical Beasts research to encompass a broad range of actors—business and operational partners, technical or analytical tool providers, and, in some cases, entities that also function as brokers or resellers.

On the other hand, **other terms carve out brokers and resellers and focus on other functions of intermediaries.** For example, infrastructure providers are characterized as entities leasing domains, hosting, or operating infrastructure to multiple vendors, providing a commoditized, reusable operational layer for multiple exploits. Access providers are described as firms or individuals that integrate exploits into tools and sell "access-as-a-service" to clients.

**The term of intermediary also takes on various meanings and implications across mentions, or lack thereof, in policy.** For example, the 2025 Pall Mall Code of Conduct uses "intermediary" explicitly, grouping "resellers, distributors, brokers, and system integrators" of commercial cyber intrusion capabilities together under a single umbrella. In contrast, the Code distinguishes another category for the role of access providers. While this represents a step toward articulating the diversity of actors in the OCC marketplace, there is little attention devoted to the functions and effects of these intermediaries. Rather, this report highlights the instances in which distinguishing between terms is beneficial to policymakers in ongoing industry code-of-practice to effectively include entities that fit more granularly within the market, bolstering potential implementation of outcomes from the code-of-practice.

On the other hand, **some policy documents do not directly mention the role that intermediaries play in the OCC marketplace.** For example, the 2023 *US State Department's Guiding Principles* focuses on government procurement, transparency, and human rights obligations of states and vendors that deploy surveillance technology. In this instance, "vendors" and "surveillance technologies" are treated as broad, catch-all categories, but the guiding principles do not specifically include brokers, resellers, infrastructure providers and the other obscure players in this ecosystem—even though these actors are drivers of price distortion, supply-chain opacity, and risk.

Finally, within the technical and threat-intelligence community, **intermediary terminology is more closely tied to specific entities in case studies:** Singaporean brokers for Indonesian spyware procurement, third-country intermediaries in Hungary, and exploit brokers or suppliers like COSEINC in Singapore or firms operating in China. Reports from these groups reference the functions that "middlemen," "brokers," "regional partners," and "local distributors" take such as repackaging, resale, and routing logistics, but often without drawing specific lines between the terms and which specific actions they take. In the industry and vendor ecosystem itself, marketing language includes "partners," and "value-added resellers," which flattens important distinctions.

There is overlap across this landscape, specific intermediaries connect entities within the OCC supply chain to support product development. Where they diverge is when and how clearly roles are named, differentiated, and assigned responsibly. Policy frameworks tend to underspecify intermediaries altogether; technical reporting documents their behavior without standardizing definitions; and industry terminology combines multiple roles under ambiguous labels. Without clarification and specificity, it is difficult to surface accounta-

3. Roundtable #1.

4. As early as 2012, RCS facilitated the sale of Hacking Team products and services, including Hacking Team's Remote Control System (RCS), to government agencies in Bangladesh, Pakistan, and Turkmenistan. In 2022, security researchers at Lookout determined RCS Lab created and sold the Hermit spyware, and it continues to operate as a spyware vendor.

bility or design effective policy to encourage market regulation. Without clear differentiation, policymakers risk applying underdeveloped, misdirected policies that may have minimal or counterintuitive effects on marketplace transparency. Therefore, disentangling the functions of these entities is a necessary step toward understanding the landscape and designing policies that address how this market functions in practice. For example, policy solutions to curb an individual operating as a broker versus a company operating as a reseller might take different approaches, with governments having their own priorities. Thus, for this piece, the authors rely on specific terms to clarify the function that each entity type(s) serves in the market and will use the term most closely aligned with an intermediary type versus a more general term such as "middlemen" or "contractor" to inform policymakers seeking to address specific characteristics of these entities.

## A note on related markets

Taking a step back from the cybersecurity marketplaces, intermediaries are observable across complex and sometimes illicit supply chains, with parallel effects on connectivity and opacity. They are key components of global supply chains ranging from diamond trade and critical minerals to commercial data brokers and the wider defense sector. Across these supply chains, intermediaries play an important role in aggregating, transforming, or legitimizing goods as they move across regulatory lines. Brokers may resemble commodity traders who arbitrage information and relationships, and there are parallels to commercial data brokers who package digital assets sources indirectly through oftentimes untraceable or illegitimate means. These commonalities highlight how the OCC marketplace similarly is characterized by multilayered supply chains and shaped by asymmetrical information and specialized labor.

These comparisons surface considerations of how, if at all, the OCC marketplace can achieve rigorous and legitimate responsible purchasing protocols for cyber capabilities. While these sectors, including entities supporting OCC development, are shaped by state and industry imposed due-diligence norms and obligations including Know Your Customer requirements, beneficial-ownership disclosures, and chain-of-custody documentation, an overall lack of vendor and intermediary reporting and transparency persists. Given this, the following section aims to fill in some of these knowledge gaps regarding the operation of and the effects posed by intermediaries in the OCC supply chain.

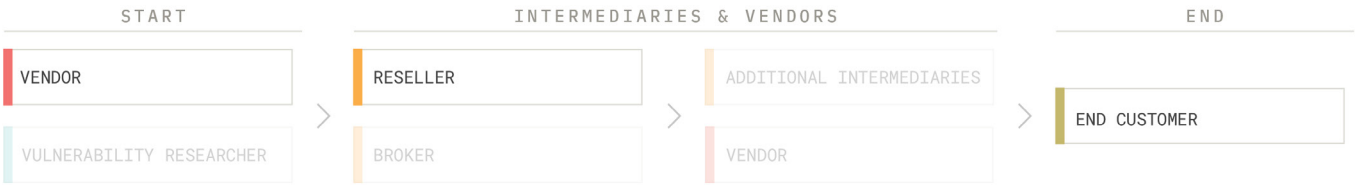
### The driving and narrowing effects of brokers and resellers on the OCC marketplace


**Fig. 1:** Effects that intermediaries have on driving and narrowing proliferation in the OCC marketplace.

This section draws on the insights from roundtables to characterize the effects brokers and resellers appear to have on the OCC marketplace. A limited body of public research has investigated the economy of vulnerability trades and exploitations, analyzed the business practices of known exploit vendors, and articulated the relationship between exploits and the spyware marketplace. In each of these cases, analyses rely on public knowledge and rare leaked documents to draw insights about the ecosystem. To compliment this and to expand the landscape of shared public knowledge, this analysis follows the methodology of recent policy research by turning to experts in a roundtable format to drive conversation and insights into underattended areas of the marketplace.

Here, effects are grouped in two major categories—features that drive proliferation of the OCC marketplace and features that narrow or limit the scope of the OCC marketplace. While these effects pose different consequences for different actors ranging from those seeking wider access to the marketplace to those seeking a far more contained and heavily regulated ecosystem, the authors frame these effects principally in terms of how brokers and resellers shape the marketplace itself. Thus, on the one hand, this analysis demonstrates that entities drive proliferation through the development, sale, and deployment of products. On the other hand, this piece observes the narrowing effects to widespread proliferation principally by driving costs, limiting the diversity of product types, and presenting roadblocks to necessary transparency and due diligence.

**Fig. 2:** Example of how a spyware vendor, like Quadream, utilizes resellers to get to specific end customers.




As detailed in the subsequent subsections, the presence of intermediaries can be characterized as both enabling proliferation and contributing to the homogeneity of the marketplace. While intermediaries fuel the proliferation of OCC, layering additional opacity into already murky supply chains, they also offer policymakers essential leverage points. Their market position, and critical functions they provide in supporting OCC deployment and transactions, make them uniquely effective targets for the needed transparency and enhanced due diligence requirements to curb the rampant proliferation of tools.

## Driving market mechanics

Emerging from expert interviews and case study compilation are three critical roles that intermediaries play in connecting entities in OCC supply chains and driving market proliferation. First, brokers and resellers facilitate sales across jurisdictions, increasing overall access to these capabilities oftentimes to new vendors or markets that otherwise could not directly procure these capabilities directly from a vendor. Second, they enable product development by providing skills, services, or pieces of an end-product that could not be easily developed inhouse by a vendor. Finally, brokers and resellers can aid with operation deployment, to assist with the hands-on tasks of using an offensive cyber capability. Notably, the authors highlight that these features are not the only enabling effects intermediaries have on OCC marketplace proliferation, but rather, there are three major trends highlighted throughout interviews and case study analysis.

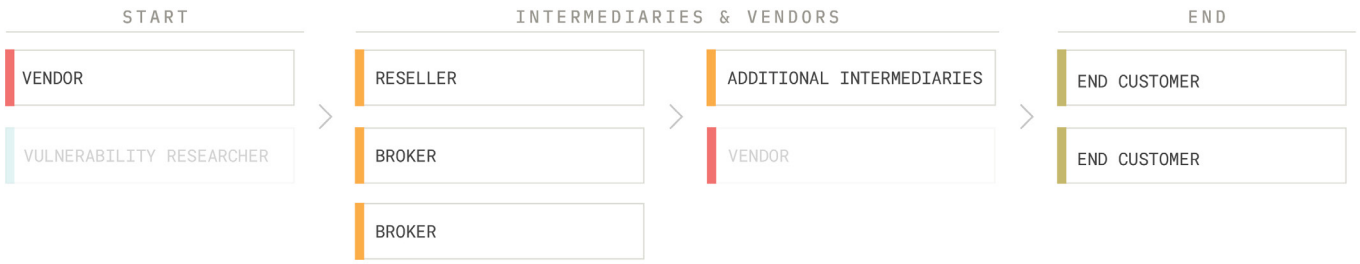
## Facilitating sales across jurisdictions

Reports from civil society suggest that brokering and reselling intermediaries have played key roles in numerous high-profile transactions. Specifically, intermediaries have facilitated transactions that otherwise could not have taken place given regional export controls or trade bans.

For example, in 2017, spyware vendor Quadream Inc. established its own reseller, InReach Technologies Limited. Sourcing revealed InReach Technologies Limited was "solely founded for the promotion of Quadream products, like Reign, outside of Israel" to bypass the EU's dual-use export.

Later, in 2018, Bangladesh acquired Israeli-made surveillance technologies through Hungarian and Thailand-based resellers to circumvent the Bangladeshi trade ban that prohibits direct trade with Israel. Without intermediaries, it is unlikely this acquisition would have occurred. Again, in 2021, Bangladesh acquired surveillance technology by relying on intermediaries. The state procured surveillance technology from the Intellexa Consortium's reseller Passitora Ltd (formerly WS WiSpear Systems Limited). The Intellexa Consortium is known for its Predator spyware. Passitora Ltd had sold its product to broker Toru Group Limited, a Swiss company operating out of the British Virgin Islands. This case highlights an example of an intermediary chain, working jointly in service of an end-use OCC vendor, which, through these multiple sales introduces additional opacity into the supply chain for these goods and services.

**Fig. 3:** Example how spyware vendors can utilize multiple brokers and resellers in a chain to get to various end customers.




Intermediaries also expand the total geographic market for spyware vendors by connecting regional markets, which might otherwise be constrained by export regulations or limited regional capacity. For example, the South African company VASTech, connected spyware vendor Hacking Team (now named Memento Labs) to sell the vendor's spyware to "local customers." Other times, as noted by roundtable participants, third-country intermediaries facilitate sales where vendors cannot or do not want to appear directly, oftentimes to avoid unwanted public attention and potential reputational harm.[5] As noted in Mythical Beasts Diving into the Depths of the Global Spyware Market, ten intermediaries (resellers) facilitated NSO Group's Pegasus sales to government buyers. Unlike the case with VASTech, Mexican intermediaries created misleading and vague contracts that concealed both the products and the original vendor, illustrating how intermediaries can be used as a tool to avoid transparency in the marketplace for OCC.

Overall, both brokers and resellers widen the reach of cyber-intrusion vendors into jurisdictions that would be otherwise inaccessible due to reputational, political, export-control, or trade barriers widening and driving the sales of these capabilities.

## Enabling product development

Throughout the expert roundtables and individual consultations, a recurring observation was that exploit brokers and resellers fill a commercial gap in the development and, ultimately, the proliferation of OCC products. Notably, experts reiterated that OCC products rarely rely on a single exploit, rather they require an interdependent chain of exploits and sometimes additional infrastructure.[6] Intermediaries meet this need by bridging the gap between security researchers and vendors seeking their exploits. In doing so, they can increase the rate of OCC development by reducing the time needed to identify and negotiate between researchers and buyers. As noted in the roundtables, successful vulnerability brokers maintain regular relationships with government entities and private contacts, thereby establishing some trust in an ecosystem reliant on reputation and word of mouth, meaning that they can more efficiently match customer demands with the current supply of vulnerabilities.[7]

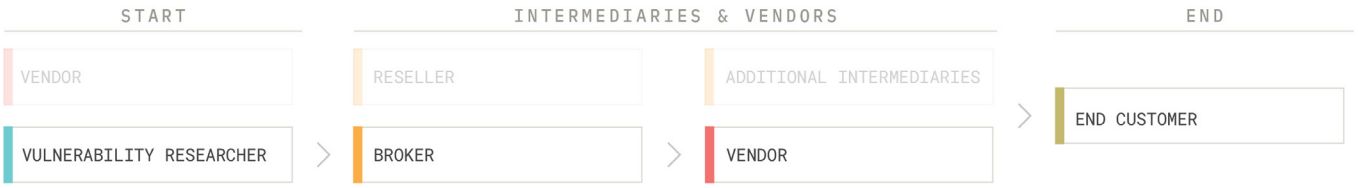
In addition to matching supply with demand, exploit brokers can bundle components of the supply chain so that vendors do not need to establish individual relationships and transactions themselves. Evidence from recent reporting suggests that brokers and resellers are meeting these product development needs not only through the sale of exploits but also by providing infrastructure setup support or by arranging transactions through platforms with limited traceability to circumvent oversight. Taken together, these entities meet a marketplace need by connecting skills, services, and products to OCC vendors who may, for a variety of reasons discussed above, seek these external services.

## Supporting operational deployment

Brokers and resellers often meet vendor needs by facilitating the transaction of infrastructure, where they provide platforms or services to assist with operational deployment of a capability. This allows OCC vendors to scale operations across multiple regions without having to rely on local infrastructure built in-house from scratch.[8] Recorded Future's analysis of Predator spyware reveals the diverse operational deployment roles that resellers fulfill, from establishing operational training centers

5. Roundtable #1; Roundtable #2 (virtual), December 16, 2025.
6. Roundtable #1.
7. Roundtable #1; Roundtable #2.
8. Roundtable #1.

**Fig. 4:** Example how vulnerability researchers can sell to brokers, like Zerodium, who then sell to vendors that package these vulnerabilities with malware to send to end customers.




to operating front companies to ship products to providing data analysis systems.

This case is especially significant, as the Intellexa Consortium—the business cluster behind Predator spyware—is renowned for incorporating intermediaries "in house." Meaning, the vendor itself owns various resellers, brokers, and infrastructure providers versus contracting them externally, suggesting that even sizeable spyware vendors that "own" various intermediaries also require external contracted intermediary support for operational deployment for certain targets.

## Limiting market proliferation

While the previous three broker and reseller effects demonstrate how these entities can meet the needs of the OCC marketplace and advance the market's proliferation, experts and case studies similarly highlighted how, on the other hand, intermediaries can contribute to increased homogeneity off the marketplace in several ways. Specifically, this includes driving up cost, limiting the diversity of product types, and impeding due diligence and transparency efforts.

## Escalating costs

Brokers and resellers, across the marketplace, anecdotally appear to drive up the final cost of OCCs. Multiple roundtable members with industry experience at many junctures of these supply chains described how each broker in a chain adds its own markup, layering on a 10-15 percent markup to the exploit for each onward sale.[9] Popular and open-access exploit marketplaces, like Zerodium, will list the prices of vulnerabilities, but what remains unclear is the extent to which these public prices reflect the intermediary markup.

Evidence suggests that the costs of exploits range drastically, with some of the most sought after exploits, like zero-click or mobile-messaging exploits being notably more expensive. Similar cost escalation occurs at other junctures in the OCC marketplace. For example, MATIC— a reseller of NSO Group's Pegasus spyware—sold Pegasus to the Polish Central Anticorruption Bureau with a nearly $1.5 million markup.

These markups exist at virtually every step of building and selling OCCs, which push higher-end capabilities out of reach for smaller states and agencies, effectively restricting market access to those with the most purchasing power. As reiterated throughout this section, brokers and resellers appear to fill an open commercial gap and charge a fee for their services. Consequently, the lack of transparency on pricing and inflation contributes to overall marketplace ambiguity for the industry as a whole by increasing opacity on costs associated with developing, selling, and procuring OCCs.

## Limiting the diversity of products

Roundtable participants noted that a consequence of both the current intermediary ecosystem and in-house vulnerability research is an overall narrowing of what is considered a top-priority commodity. With buyers' focus on the most popular target vectors (such as iOS and Android devices) and on final products that prioritize speed, timing, precision, and anonymity, downstream intermediaries respond by focusing their discovery and procurement on these few, high-value exploits.[10]

These experts narrowed in on this unintended market effect, in which buyers seek out and buy certain vulnerabilities (i.e., remote bypass for popular operating systems), which contributes to knock-on effects for the wider intermediary marketplace. Roundtable participants explained that as resellers and brokers prioritize acquiring these few high-value exploits, there is limited buyer interest and purchasing power for smaller bugs that can be used in complimentary or alternative ways

9. Roundtable #1.
10. Roundtable #2.

to reach similar end goals.[11] In essence, while it is not possible to have full view into the demand-and supply-side activities, "all eyes are trained on the same targets."[12] One participant noted an exception to this marketplace norm, highlighting a positive externality in the public-private ecosystem in Israel that has created an incentive system in which researchers and intermediaries have access to funding and investments necessary to create and prove product viability for OCCs that exploit less or obvious sources.[13]

What was observed, in general, is that most of the attention and purchasing power is directed at a relatively narrow slice of the vulnerability marketplace to build out the exploit chains of OCC products. Experts speculated on the consequences of this intermediary and product homogenization. For instance, they highlighted that from an engineering perspective, products appear to be "less creative." Others noted that this zeroing in on the same few exploits incentivizes brokers and resellers to engage in disreputable and insecure business practices such as selling the same exploit to different vendors, threatening security breaches or bottlenecks when exploits are discovered and patched.

## Impeding transparency and due diligence

Overall, the introduction of more actors in the form of intermediaries to the OCC ecosystem poses additional considerations to the tracking and reporting necessary for transparency initiatives. Given the relationship-based nature of brokering and reselling, where deals and transactions oftentimes rest on preexisting, trusted contacts or references, the ability to surface and track these transactions within a digital "supply chain" is limited.[14] This has implications for the growing advocacy and policy guidelines for which "responsible purchasing" has been offered as a potential remedy to market proliferation.

The analyses above highlight how brokers and resellers can drive-down transparency efforts in the marketplace for OCC by muddying supply chains and creating confusion for end-buyers as to the source of a product or product component, which in turn complicates due-diligence efforts and "responsible purchasing." Even vendors of OCCs have indicated how intermediaries complicate their own alleged due-diligence efforts. For example, the CEO of spyware vendor Memento Labs, recently asserted that one of its clients misused outdated variants of their malware. This demonstrates that OCC vendors can lose control of variant propagation once intermediaries and resellers are involved. Members of the industry echoed this sentiment, describing the "ceiling of capabilities" problem—as resold or outdated capabilities continue to circulate in the market, sometimes through third-country intermediaries, the likelihood of detection increases and the effectiveness of the exploit is reduced.[15] On the other hand, current market opacity enables unchecked vendor transparency reports, including the recent 2025 NSO transparency report, which lacks any concrete details on annual disclosures, supply chains, customers, and more.

Further complicating transparency and due diligence efforts are incentive structures in the marketplace for OCC. Emerging security researchers and brokers are often incentivized by the appealingly sizable and rapid profit potential, shifting the focus to speed and margin overdue diligence obligations. Discovering and selling vulnerabilities is not geographically restricted to certain markets and thus the profit margins can be "transformative" for some researchers and intermediaries, particularly in the global majority.[16]

An ultimately observable theme in the OCC supply chain, like many other illicit flows, is that entities are largely incentivized by factors including profit and reputational protection, which oftentimes are measured by high levels of discretion and privacy. As a consequence, supply chain transparency and publicly accessible and meaningful due diligence contrasts with these appealing payouts and an inherent culture of opacity.

11. Roundtable #2.
12. Roundtable #2.
13. Roundtable #2.
14. Roundtable #1; Roundtable #2.
15. Roundtable #1.
16. Roundtable #1.

## Policy recommendations

The policy recommendations below aim to address the aforementioned effects that brokers, resellers, and other intermediary types pose. Based on analysis from interviews and background research, this report sets out four recommendations aimed at confronting the consistent issue set across the Mythical Beasts project—increasing and incentivizing transparency at multiple levels of the OCC supply chain.

These specific recommendations are oriented toward governance regimes in the United States, the United Kingdom, and the multilateral Pall Mall Process to develop Know Your Intermediary requirements, improve corporate registries to capture more details about intermediary relationships, and create certification programs.

### I. Implement Know Your Vendor requirements

To facilitate more effective due diligence of cyber capability transactions, governments should gain a better understanding of brokers and resellers enabling these transactions. Know Your Vendor requirements would mandate that OCC brokers and resellers disclose their supplier relationships, vendor partnerships, investors, subcontractors, and parent entities to develop a consistent reporting environment where government licensing officers can assess whether prospective intermediaries have ties to sanctioned or restricted entities before signing contracts.

Within the United States, the Federal Acquisition Regulatory Council should update the Federal

Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and Defense Logistics Acquisition Directive to require any broker or reseller bidding on government cyber operations contracts to disclose vendor relationships, supplier networks, investors, subcontractors, and holding entities. While the Defense Logistics Acquisition Directive requires the disclosure of "the name and location of all supply chain intermediaries," it does not require information about access providers, parent companies and holding companies, investors, and others.

Within the United Kingdom, the Cabinet Office should update procurement regulations to require intermediaries providing spyware-related services to disclose complete supply chains.

### II. Improve corporate-run registries for brokers and resellers

Government-run corporate registries are essential resources for due diligence and accountability in tracking OCC behavior. As indicated in the Mythical Beasts project series, there is work to be done to ensure these registries are comprehensive, publicly accessible, and contain verified information to bolster transparency and accountability efforts.

National regulations should determine comprehensive requirements for brokering and reselling related entities in corporate registries. At minimum, registries should include:

- **Basic company information:** Name, registration number, tax ID, address, contact details, and date of registration
- **Ownership details:** Senior executives, management board, beneficial owners, and investors
- **Operational details:** Number of employees, geographic scope of operations, and jurisdictions where licensed to operate
- **Corporate history:** Name changes, mergers and acquisitions, and predecessor entities

This information serves as a baseline but could be expanded to include relationships with known spyware manufacturers, telecommunications partners, and access providers.

Within the United States, there is no centralized "nationwide" corporate registry, as each state maintains their own. The National Association of Secretaries of States can build out guidance on what individual states can do to bolster disclosure requirements of dual-use technology companies on their respective registries, which will more holistically capture information about brokers and resellers.

By contrast, the United Kingdom has a more robust corporate registry system. Nevertheless, to improve this system to capture additional information about OCC intermediaries, the United Kingdom should encourage Parliament to amend the Companies Act 2006 to include additional information about entities connected via supply chains in the national registration. When it comes to international fora, the United Kingdom, through the Pall Mall Process, should establish a Working Group with Code of Practice signatories on how states can improve corporate registries to better capture information pertinent to intermediary and OCC marketplace behavior. The UK government should also consult civil society organizations to provide expertise through this process.

### III. Certified brokers and resellers programs

As leaders of the Pall Mall Process, the United Kingdom and France should establish internal certification programs recognizing brokers and resellers that demonstrate exceptional compliance practices and encourage other signatories to the Pall Mall Process Code of Practice for States to do the same. Utilizing the Pall Mall Code of Practice for industry as a jumping off point to establish a certification, certified brokers and resellers are eligible to receive streamlined licensing processes for low-risk transactions and have a greater likelihood of winning government contracts, encouraging other brokers and resellers in the ecosystem to pursue this certification. This recommendation is a voluntary certification program, where interested brokers and resellers can apply to be certified for the benefits overviewed above, as not every broker and reseller seeks to work directly with government clients. Certification criteria must include a government-led due diligence effort to ensure a demonstrated history of accurate disclosure, implementation of human rights impact assessments, participation in industry best practice fora, cooperation with government due diligence investigations, and consultation with civil society actors. More detail on assessment of these criteria is below.

Within the United States, Bureau of Industry and Security (BIS) should administer the certification program, serving as the entity that issues, maintains, and revokes certifications. Shoring up technical expertise will enable BIS to leverage its existing expertise as the entity that oversees export controls of dual-use goods that pose potential risks to national security and can evaluate compliance through access to export violation records and licensing records. BIS can also enforce compliance, as it already oversees the "Export Controls List" on which some OCC vendors are listed.

The US Department of State should coordinate and share human rights impact assessments for certification applicants, providing country and regional human rights risk assessments, and compliance with international law. This can be informed through expert consultation by civil society organizations to review and bolster the rigor of the assessment's methodology and focus. Finally, the Office of Foreign Assets Control at the US Department of the Treasury should provide sanction screening and verification services for the certification program.

In the United Kingdom, the Export Control Joint Unit (ECJU) within the Department for Business and Trade should administer the certification program, serving as the entity that issues, maintains, and revokes certifications. The ECJU, similar to BIS, can leverage its existing expertise in UK export control regulations and licensing requirements to implement and oversee this program.

The Foreign Commonwealth Development Office, similar to the US Department of State, should coordinate and share human rights impact assessments for certification applicants, providing country and regional human rights risk assessments, compliance with international law, and adherence to UK human rights commitments and the Consolidated EU and National Arms Export Licensing Criteria. Finally, the Office of Financial Sanctions Implementation of His Majesty's Treasury can administer UK sanctions screenings and compliance verifications for the certification program.

Information sharing, coordination, and harmonization between various intermediary certification programs in the United States and the United Kingdom can be coordinated during the Pall Mall Process or other appropriate international fora.

## Conclusion

The opacity of intermediaries in the OCC marketplace represents a discernable gap in current policy frameworks. This research demonstrates how intermediaries—be it brokers, resellers, or other entities—are essential enablers and connectors of the OCC supply chain. They drive proliferation by expanding market access across jurisdictions, supporting product development, and facilitating operational deployment while introducing market complications through cost escalation, product homogenization, and supply chain obfuscation.

The policy recommendations highlighted in this piece reinforce a core point—transparency. They seek to bolster publicly accountably transparency without pushing legitimate vulnerability research underground. These recommendations recognize and reflect on treating intermediary roles in OCC marketplace not as a collective unit, but rather as distinct categories with a range of policy responses.

When journalists, political leaders, activists, and private citizens become targets of OCCs like spyware that has been developed through intermediary chains, the opacity complicates accountability and enables ongoing surveillance of personal information and private communication. Each layer of the supply chain makes it increasingly complicated to trace the technology and sales, further complicating accountability. Adding to this, intermediaries can create vulnerabilities for national security when states are unknowingly reliant on adversarial infrastructure or indirectly funding, through acquisition of these capabilities', adversarial vendors.

Through international momentum via the Pall Mall Process and the wide variety of politic actions to curb the proliferation and misuse of spyware and other OCC, a critical window exists to shape the future of intermediaries' operations within the OCC supply chain and bring them out from the shadows.

## About the author

**Jen Roberts** is an associate director with the Cyber Statecraft Initiative, part of the Atlantic Council's Tech Programs. Roberts leads CSI's Proliferation of Offensive Cyber Capabilities work, including the management of the Mythical Beasts project series. Roberts holds an MA in International Relations and Economics from Johns Hopkins University's School of Advanced International Studies (SAIS) and a BA in International Studies from American University's School of International Service.

**Sarah Graham** is a nonresident fellow with the Cyber Statecraft Initiative, part of the Atlantic Council's Tech Programs. She is also a European Union Schuman Fulbright fellow working with the Center for Democracy and Technology in Brussels. Her work focuses on European digital policies and how they might respond to intrusive and harmful uses of technologies ranging from spyware to digital platforms. Graham is also a policy research affiliate at New York University's Center for Social Media and Politics, where she previously served as the Center's research and operations manager and oversaw a diverse portfolio of projects and data access initiatives for interdisciplinary research teams. She has contributed to publications at the *Journal of Experimental Political Science* and *Journal of Quantitative Description,* and her writing has appeared in Brookings and Tech Policy Press. She holds degrees from the University of St. Andrews and New York University.

**Lyla Renwick-Archibold** is a research associate in Artificial Intelligence at the Council on Foreign Relations. Renwick-Archibold previously interned at the Atlantic Council's Cyber Statecraft Initiative, where she researched the spyware market. She also served as a Princeton in Africa Fellow based in Tanzania, where she led digital literacy and tech education initiatives in partnership with schools and local organizations. She graduated from Washington University in St. Louis with a degree in computer science, where she focused on the intersection of technology, policy, and equity. Renwick-Archibold has worked in research and product roles across the public, private, and nonprofit sectors. She served as a researcher for Coda Media, where she reported on AI, surveillance, and human rights in East Africa. Before that, at the Surveillance Technology Oversight Project, she published articles on facial recognition and digital surveillance.

*Acknowledgments*

*The authors owe a debt of gratitude to the security research community, particularly to the individuals who spoke candidly about their many years of learned experiences during our roundtables and in interviews; the report authors are eternally grateful.*

*Thank you to Winnona DeSombre Bernsen and Nikita Shah, whose valuable conversations shaped the early focus of this issue brief. To all who have contributed to the Mythical Beasts projects over the years, this project would not be the same without your valuable contributions.*

## About the center

The **Cyber Statecraft Initiative** works at the nexus of geopolitics, technology, and security to craft strategies to help shape the conduct of statecraft and to better inform and secure users. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.



Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org