Atlantic Council

SCHOOL of INTERNATIONAL SERVICE
AMERICAN UNIVERSITY • WASHINGTON, DC

CYBER STATECRAFT
INITIATIVE

MARKETS MATTER:
A Glance into the Spyware Industry

by Jen Roberts, Trey Herr,
Emma Taylor, and Nitansha Bansal

Atlantic Council

CYBER STATECRAFT INITIATIVE

SCHOOL of INTERNATIONAL SERVICE
AMERICAN UNIVERSITY • WASHINGTON, DC

The **Cyber Statecraft Initiative**, part of the Atlantic Council Tech Programs, works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. 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.

American University's School of International Service (SIS) is a top-10 school of international affairs located in Washington, DC. Since our founding in 1957, we have answered President Dwight D. Eisenhower's call to prepare students of international affairs to "wage peace." We do so because the world needs capable, service-minded leaders ready to make a positive change in our world. Our world-renowned faculty—leading political scientists, economists, sociologists, anthropologists, demographers, geographers, historians, and experts in national security, international development, global health, communications, energy, and the environment – produce meaningful, transformational research. They impart their experience, knowledge, and skills to more than 3,000 graduate and undergraduate students annually and prepare students for global careers in government, nonprofits, and business around the world.

Authors
Jen Roberts, Trey Herr, Emma Taylor, and Nitansha Bansal

Editor
Samia Yakub

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

April 2024

Design by: Donald Partyka and Anais Gonzalez

Cover: Iswanto Arif

Atlantic Council

SCHOOL of INTERNATIONAL SERVICE
AMERICAN UNIVERSITY • WASHINGTON, DC

CYBER STATECRAFT
INITIATIVE

MARKETS MATTER:
A Glance into the Spyware Industry

by Jen Roberts, Trey Herr,
Emma Taylor, and Nitansha Bansal

Table Of Contents

Executive Summary

The Intellexa Consortium, a complex web of holding companies and vendors for spyware and related services, have been the subject of recent, extensive sanctions by the US Department of the Treasury and the focus of reporting by the European Investigative Collaborations among others. The Consortium represents a compelling example of spyware vendors in the context of the market in which they operate—one which helps facilitate the commercial sale of software driving both human rights and national security risk.[1] This paper addresses an international policy effort among US partners and allies, led by the French and British governments, as well as a surge of US policy attention to address the proliferation of this spyware. This paper offers a case study of the Intellexa Consortium, based on public records and open source reporting, as an argument for policymakers to consider the wider network of investors and counterparties present in this market rather than constraining their focus on individual vendors. This consortium showcases many of the trends observed in how other spyware vendors organize, straddle jurisdictions, and create overlapping ownership structures. This paper argues that policymakers must approach the market as a whole, a large and complex but interlinked system, in designing future policy interventions against these vendors and their respective supply chains. In closing, the paper offers several tangible impacts and insights into this market, calling for greater transparency writ large, but also for increased attention into the individuals and investors that facilitate the proliferation of spyware.

Introduction

For decades, private companies have developed, sold, and maintained software to steal digital data from computing devices and sell it to others—eroding the notion that digital espionage is an activity limited to governments. Mobile phones and their operating systems have been an especially popular target as, in many ways, the devices are a slickly packaged espionage party pack of microphones, cameras, Global Positioning System (GPS), and cell network location transmitters, with the applications to obtain sensitive personal data like messaging and contacts. The customers for this software-enabled spying are myriad, including law enforcement, domestic security, and intelligence organizations across the globe. Spyware has garnered international attention due to some governments' utilization of the software to violate human rights and for its use in internal surveillance and policing, as well as larger national security risk in transferring offensive cyber capabilities to states without means to provide lawful oversight and democratic input on their use.

In the decades that this spyware has been built and sold, profiles have been written about as many as a dozen vendors. Reports from companies like Google,[2] Meta,[3] civil society champions Amnesty International[4] and the Citizen Lab[5], and news outlets like Reuters[6] and *Forbes,*[7] as well as

1 US Department of the Treasury, "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium," March 5, 2024, https://home.treasury.gov/news/press-releases/jy2155; "Predator Files: How European Companies Supplied Dictators Cyber-Surveillance Tools for More than a Decade," European Investigative Collaborations, accessed April 10, 2024, https://eic.network/projects/predator-files.html.

2 "Buying Spying: Insights into Commercial Spyware Vendors," *Google Threat Analysis Group*, February 6, 2024, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf.

3 AJ Vicens,"Meta Details Actions Against Eight Spyware Firms," *Cyberscoop,* February 14, 2024, https://cyberscoop.com/meta-details-actions-against-eight-spyware-firms/.

4 Amnesty International, *The Predator Files: Caught in the Net*, October 9, 2023, https://www.amnesty.org/en/documents/act10/7245/2023/en/.

5 Bill Marczak et al., "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox AD Mercenary Spyware," *The Citizen Lab,* December 16, 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-Cytrox AD-mercenary-spyware/.

6 Christopher Bing, "U.S. Slaps Sanctions on Greek Spyware Vendor, Says it Targeted U.S. officials," Reuters, March 5, 2024, https://www.reuters.com/technology/cybersecurity/us-slaps-sanctions-greek-spyware-vendor-says-it-targeted-us-officials-2024-03-05/.

7 Thomas Brewster, "A Multimillionaire Surveillance Dealer Steps out of the Shadows … And His $9 Million WhatsApp Hacking Van," *Forbes,* April 5, 2019, https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/?sh=70e4bcfd31b7.

the Atlantic Council,[8] have examined the behavior of these companies, the services they sell, and the corresponding harm that software can pose.

But absent from most of this analysis, save some at the edges of industry and academia, is an accurate picture of these vendors as a whole market—one in which firms conduct business under multiple names, work with investors across the globe, and where webs of interpersonal relationships underpin a shifting roster of corporate names and titles. These factors have hampered policy efforts to extract transparency from this market and limit the sale and use of spyware.

Recently, the US government took policy action to target specific firms and several named individuals developing and selling this software. In March 2024, the Treasury Department sanctioned the Intellexa Consortium, profiled in more detail in this brief, following the listing of several vendors by the Department of Commerce in 2023.[9] Together with policy efforts like those in the UK-and-French-led Pall Mall process[10] launched in February 2024 and the widely discussed but ultimately inconclusive PEGA Committee,[11] which the European Parliament convened in 2023, there has been a sharp increase in interest from governments in the activities of this market and their potential for harm.

Figure 1: Groups Targeted by Spyware

8 Winnona DeSombre et al., *Counter Cyber Proliferation: Zeroing in on Access-as-a-Service, Atlantic Council,* March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

9 US Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," November 3, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

10 Sven Herpig and Alexandra Paulus, "The Pall Mall Process on Cyber Intrusion Capabilities," *Lawfare,* March 19, 2024, https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities.

11 "European Parliament Draft Recommendation to the Council and the Commission Following the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware," *European Parliament,* May 22, 2023, https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html.

Policy that addresses these vendors and their major financial and supplier relationships within this market will be more impactful than targeting single vendors alone. To sharpen the emerging government efforts mentioned above, this paper presents a case study of the Intellexa Consortium and its investor and subsidiary ties as a prototype of analysis focusing on a vendor's relationship to this wider spyware market, in addition to their own activities.

In the pages that follow, the paper offers some basic definitions and examines previously reported and open source information about the specific case of the Intellexa Consortium, which recent US Treasury actions highlighted. Sanctions are particularly useful in targeting individuals across multiple jurisdictions and companies, and this is the first time the US has used this policy lever against a spyware vendor.[12] The case study summarizes the corporate entities, investors, and founders that make up this consortium along with key public business relationships and how those relationships have evolved over time. Finally, the paper highlights several features of the Intellexa Consortium organization and implications for policy.[13] This is just one case study, but it demonstrates a model for what is possible in a more holistic analysis of the spyware market and the utility of that approach to policymakers, researchers, and advocates alike.

Terms of Debate

This section offers definitions for some key terms as applied in this work and present in many others as a way of scoping the analysis. Policymaking around spyware has suffered in the past due to unclear terminology and inconsistent definitions. Recognizing the significant energy present across international policymaking efforts like the Pall Mall process, this section seeks to better specify terms of an ongoing debate. The authors submit these terms as analytically useful to the purpose, concise, and sufficiently rigorous so as to capture much of the discussion happening in the seams and gaps between both policymaking and information security research communities.

Spyware

Spyware is a type of malware[14] that facilitates unauthorized remote access to an internet-enabled target device for purposes of surveillance or data extraction. Spyware is sometimes referred to as "commercial intrusion [or] surveillance software," with effectively the same meaning. Spyware works without willing consent of the target or anyone with access to their device; thus, this paper does not consider the market for so-called 'stalkerware,' which generally requires interaction from a spouse, partner, or someone else with access to a user's device. This definition also excludes software that never gains access to a target device, such as surveillance technologies that collect information on data moving between devices over wire (i.e., packet inspection or 'sniffing') or wireless connections. This definition also excludes hardware such as mobile intercept devices known as IMSI-catchers, or any product requiring physical access to a target device such as forensics tools.[15]

This definition is limited, by design, to disentangle the lumping of various other surveillance toolsets into the definition of spyware.[16] Hardware devices require physical device access that adheres to jurisdiction-specific

12 Christopher Bing, "U.S. Slaps Sanctions on Greek Spyware Vendor, Says it Targeted U.S. officials," Reuters, March 5, 2024, https://www.reuters.com/technology/cybersecurity/us-slaps-sanctions-greek-spyware-vendor-says-it-targeted-us-officials-2024-03-05/.

13 Andrew Selsky, "Oregon Examines Spyware Investment amid Controversy," *OPB*, August 5, 2021, https://www.opb.org/article/2021/08/05/oregon-examines-spyware-investment-amid-controversy/; Stephanie Kirchgaessner, "US Announces New Restrictions to Curb Global Spyware Industry," *The Guardian*, February 5, 2024, https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions; Nomaan Merchant, "Victims of NSO's Pegasus Spyware Warn It Could Be Used to Target US," *The Times of Israel,* July 28, 2022, https://www.timesofisrael.com/victims-of-nsos-pegasus-spyware-warn-it-could-be-used-to-target-us/; Miles Kenyon, "Reported Blackstone NSO Deal Failure and the Risks of Investing in Spyware Companies," *The Citizen Lab*, August 15, 2017, https://citizenlab.ca/2017/08/reported-blackstone-nso-deal-failure-risks-investing-spyware-companies/.

14 "Spyware," United States Computer Emergency Readiness Team, updated October 2008, https://www.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf.

15 Also referred to as 'Stingrays' after the Harris Corporation's eponymous product line; Amanda Levendowski, "Trademarks as Surveillance Technology," *Georgetown University Law Center,* 2021, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3455&context=facpub.

16 This paper's scope is slightly wider than spyware, owing to the activities of several firms in the Intellexa Consortium, as discussed briefly below.

regulations. Passive surveillance technologies intercept and monitor communications using a broad set of tools, often in some combination of hardware and software technologies and frequently without requirement for preexisting knowledge of a target.[17]

"Commercial" Spyware?

The term spyware often becomes a proxy debate for the scope of policy. Varying definitions attempt to embed conditions as to the source or legitimacy of these software. The debate over what constitutes a legitimate use, and the channel to acquire spyware is ongoing. To avoid confusion in both analysis and policy—the authors do not embed the term "commercial" in this definition (e.g. "commercial spyware," more on this below). Spyware defines a set of technical capabilities, wherever those might be acquired. Policy addressing the "market" for spyware necessarily supposes a commercial source rather than those developed within government organizations.

Vendor

A spyware vendor is a commercial entity that develops, supports, and sells spyware to an end user. This development and support can include vulnerability research and exploit development, malware payload development, technical command and control, operational management, and training and support, but need not include all.[18] To limit discussion of spyware vendors to only those offering 'end-to-end' capabilities would risk obscuring critical commercial relationships significant to this discussion, as will become clear in the Intellexa Consortium case below.

Holding Company

Several of the vendors in the Intellexa Consortium are part of one or several holding companies. A holding company is a type of business entity whose sole purpose is to own a controlling interest in other companies.[19] These companies control subsidiaries. Rather than produce a good or supply a service, the functionality of a holding company is often tied to its ownership of its subsidiaries. Holding companies might provide oversight for subsidiaries; however, they are not involved in daily operations and remain protected from financial losses that might implicate subsidiaries.[20]

Supplier

A supplier sells a component or service in support of a spyware service to other suppliers and vendors but does not develop or operate a spyware service or work directly with end users. In common parlance, vendors can be suppliers. Here the authors focus suppliers on those firms enabling the activity of spyware vendors but without any capacity to build or sell comparable surveillance services. For example, a supplier might sell a vulnerability or a subscription of exploits to a spyware vendor or establish a service relationship. A supplier helps with the operation of a service rather than providing that service directly. Suppliers are a crucial but often underlooked part of this market. Those vendors that cannot develop some part of a spyware service in-house—most often the regular supply of software exploits needed for continued access to major operating systems—look to procure these capabilities from a supplier, which can help drive proliferation of spyware through an even more diverse market.

A Question of Scope

The definition of spyware offered here does not describe the full scope of the case study to follow. While this paper is concerned with the Intellexa Consortium and its sale of spyware, this collection of firms includes several that sell services complementary to spyware to steal credentials and surveil wireless networks. The case study of the Intellexa Consortium here is motivated by the sale and use of spyware, but does not necessarily limit its consideration of vendors and suppliers of that product.

A related, and important, issue of scope is the particular policy problem that the spyware market presents. As we have noted in previous work, "The proliferation of offensive cyber capabilities (OCC)—the combination of tools, vulnerabilities, and skills, including technical, organizational, and individual capacities used to conduct offensive cyber operations—presents an expanding set of risks to states and challenges commitments to protect openness, security, and stability in cyberspace. The profusion of commercial OCC

17 In the United States, Democratic Senator Ron Wyden of Oregon has advocated for the overhaul of Signaling System 7 (SS7), an international telecommunications protocol containing known vulnerabilities that can be exploited to provide passive surveillance capabilities; see https://www.bloomberg.com/news/articles/2024-02-29/senator-demands-overhaul-of-telecom-security-to-curb-abuses.

18 Winnona DeSombre et al., *A primer on the proliferation of offensive cyber capabilities, Atlantic Council,* March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.

19 Amy Fontinelle, "Holding Company: What It Is, Advantages and Disadvantages," *Investopedia*, February 13, 2024, https://www.investopedia.com/terms/h/holdingcompany.asp.

20 Fontinelle, "Holding Company."

vendors, left unregulated and ill-observed, poses national security and human rights risks. For states that have strong OCC programs, proliferation of spyware to state adversaries or certain non-state actors can be a threat to immediate security interests, long term intelligence advantage, and the feasibility of mounting an effective defense on behalf of less capable private companies and vulnerable populations. The acquisition of OCC by a current or potential adversary makes them more capable."[21]

Many human rights violations associated with OCC occur in the context of their use for national security purposes (e.g., by state intelligence agencies). This dichotomy illustrates the diverse set of risks that the proliferation of OCC pose. These risks include what Lin and Trachtman term "vertical" uses (by states against their own populations) and "diagonal" uses (against the population of other states, including diaspora).[22] In some cases, these capabilities are deployed intentionally, through commercial transactions or disclosure, and in other cases without intention; for example, the 'breakout' of "capabilities like EternalBlue, allegedly engineered by the United States, have already been used by the Russian, North Korean, and Chinese governments."[23]

This piece focuses on a subset of these capabilities, spyware, through a case study within the spyware market. That focus does not suggest that harm from the use of spyware is derived from their commercial sale or development outside government institutions. The commercial vendors of spyware may be the more unpredictable and less constrained source of intentional proliferation today, but they are far from the only source of harm and insecurity. Policy that seeks only to mitigate harms from the commercial sale of these capabilities risks ignoring its wider harms from a variety of sources. Commercial sale is a poor proxy for 'responsible' or 'mature' use of offensive cyber capabilities and history has shown that this market is only one, intentional part of this wider proliferation problem. Pinning policy activity on an assumption that states that can develop their own capabilities are deemed 'responsible,' and those that must resort to the open market are not, risks undermining even well-intentioned policy despite what it might offer in crafting consensus at home or abroad.

Intellexa: Behind the Music

How do these terms work in practice and what does a spyware vendor look like in 2024? This section reviews the case of Intellexa Consortium, a group of companies that has reportedly sold spyware to customers in Armenia, Colombia, Côte d'Ivoire, Egypt, Germany, Greece, Oman, the Philippines, Saudi Arabia, Serbia, and Vietnam, in addition to other countries "around the globe."[24, 25, 26] The service has also been used to covertly surveil US government officials, journalists, and policy experts.[27]

The Intellexa Consortium is made up of two main groups, Intellexa Group and Intellexa Alliance. Intellexa Group is comprised of four known subcompanies, each of which specializes to complement one another, and houses the developer of the consortium's spyware. The Intellexa

21 Winnona DeSombre et al. *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service*, *Atlantic Council,* May 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

22 Herb Lin and Joel P. Trachtman, "Using International Export Controls to Bolster Cyber Defenses," Protecting Civilian Institutions and Infrastructure from Cyber Operations: Designing International Law and Organizations," *Center for International Law and Governance, Tufts University*, September 10, 2018, https://sites.tufts.edu/cilg/files/2018/09/exportcontrolsdraftsm.pdf.

23 Winnona DeSombre et al. *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service*, *Atlantic Council,* May 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/; Gil Baram, "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat," *Council on Foreign Relations* (blog), June 19, 2018, https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat; Insikt Group, "Chinese and Russian Cyber Communities Dig Into Malware From April Shadow Brokers Release," *Recorded Future* (blog), April 25, 2017, https://www.recordedfuture.com/shadow-brokers-malware-release/; Leo Varela, "EternalBlue: Metasploit Module for MS17-010," *Rapid7* (blog), May 19, 2017, https://blog.rapid7.com/2017/05/20/metasploit-the-power-of-the-community-and-eternalblue/.

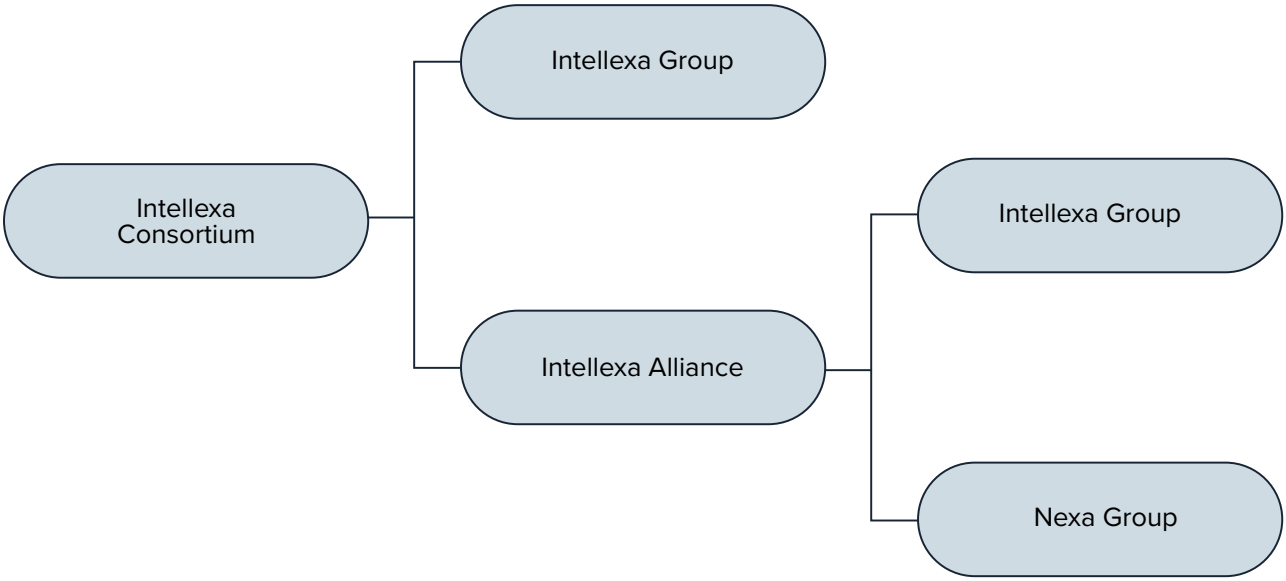
24 David Agranovich, Mike Dvilyanski, and Nathaniel Gleicher, *Threat Report on the Surveillance-for-Hire Industry,* Meta, December 16, 2021, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

25 Marczak et al., "Pegasus vs. Predator."

26 Amnesty International, *Predator Files*.

27 United States Department of the Treasury, "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium," March 5, 2024, https://home.treasury.gov/news/press-releases/jy2155.

Figure 2: Chart of the Intellexa Consortium and Subsequent Groupings



Alliance is a partnership between the Intellexa Group and the Nexa Group, a cluster of five other companies.

The phrase "Intellexa Consortium" is an analytical term that researchers and policymakers[28] have used to describe this collection of companies with close ties, apparent commercial partnerships, and comingled owners. Although both Intellexa Group and Intellexa Alliance are part of the Intellexa Consortium, neither are registered legal entities in any of the jurisdictions surveyed for this paper. Meanwhile, known entities that bear Intellexa's name, Intellexa S.A. is registered in Greece,[29] and Intellexa Limited is registered in the British Virgin Islands[30] and Ireland.[31] Part of what makes Intellexa Group unusual is this collection of customer-facing support and marketing to amplify the reach and efficacy of their services. The corporate infrastructure of Intellexa Group is configured similarly and some of these companies share common ownership. For example, Tal Dilian founded both WS WiSpear Systems Limited and Intellexa S.A. and operated the two firms simultaneously.[32]

Each of the Intellexa Group companies have a business relationship with many other entities in the group and many share the "Intellexa" name in some fashion. Intellexa Group, with or through one of the companies in the cluster, is responsible for the sale and support of the Predator spyware service.[33] Predator is a spyware service engineered to infiltrate, monitor, and steal data from a target device. Predator installation occurs via "zero-click" or "one-click" infections. One form of zero-click infection takes place when a victim's mobile browser secretly redirects to a malicious website.[34] Alternatively, one-click infections

28 "Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware," *European Parliament,* May 22, 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf; "Amendments 241-510 Draft report," *European Parliament,* January 1, 2023, https://www.europarl.europa.eu/doceo/document/PEGA-AM-740916_EN.pdf; US Department of the Treasury, "Treasury Sanctions Members."

29 "Intellexa Company," Athens Chamber of Commerce and Industry, accessed March 22, 2024, https://directory.acci.gr/companies/details/140944573.

30 "Intellexa Ltd., British Virgin Islands," *Dato Capital,* https://www.datocapital.vg/companies/Intellexa-Ltd.html.

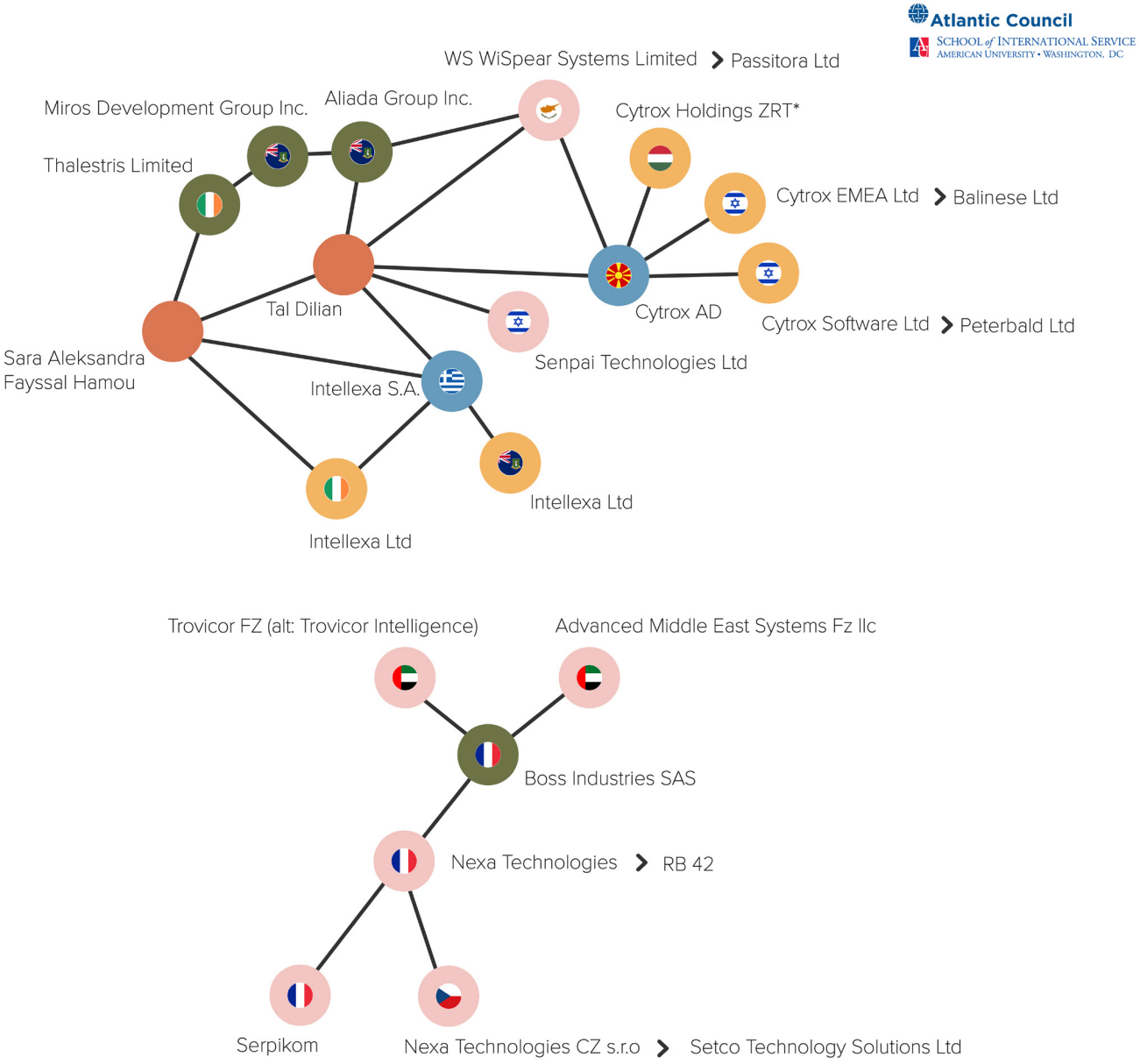
31 "Intellexa Limited," *Companies Registration Office Ireland*, accessed March 22, 2024, https://core.cro.ie/e-commerce/company/697890.

32 "Briefing for the PEGA Mission to Cyprus and Greece," *European Parliament,* October 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/738330/IPOL_STU(2022)738330_EN.pdf.

33 Amnesty International, *Global: 'Predator Files' Investigation Reveals Catastrophic Failure to Regulate Surveillance Trade*, October 5, 2023, https://securitylab.amnesty.org/latest/2023/10/global-predator-files-investigation-reveals-catastrophic-failure-to-regulate-surveillance-trade/; "Read the Intellexa Pitch on Its Spyware Tool," *The New York Time*s, December 8, 2022, https://www.nytimes.com/interactive/2022/12/08/us/politics/intellexa-commercial-proposal.html?searchResultPosition=1; Bill Marczak et al., "Pegasus vs. Predator."

34 Bill Marczak et al. "Predator in the Wires: Ahmed Eltantawy Targeted with Predator, *The Citizen Lab*, September 22, 2023, https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/.

Figure 3: Known Companies and Groupings that Comprise the Intellexa Alliance



*Cytrox Holdings Zartkoruen Mukodo Reszvenytarsasag

c. 2023

require that victims unknowingly click on a malicious link, such as an article posted to X (formerly Twitter), which the user believed to be a legitimate website.[35] After installation, Predator provides remote access to monitor the target device, manipulate local microphones and cameras, and extract data, including files, messages, and location information. Predator has been sold to states that have used it to commit human rights abuses.[36]

Intellexa Group is also part of the broader Intellexa Alliance, in partnership with Nexa Group, a consortium of four known different companies.

Reporting has often conflated these two separate clusters, identifying them as a unified entity instead of the set Intellexa *Group* and superset Intellexa *Alliance* (together with Nexa Group). This distinction is important as it helps to disentangle the complicated corporate structure and create more effective policy that targets specific clusters. The overlapping corporate structures found here are an extreme example of otherwise common trends found throughout the spyware market covering more than thirty firms with similarly named subsidiaries and nested investor and partner relationships. The figure below highlights features of the Intellexa Group and the Intellexa Alliance to clarify the operations of each association and recommend policy actions based on emerging market phenomena.

Intellexa Group

Intellexa Group's story starts with its founder Tal Dilian. Dilian was sanctioned by the US Treasury Department in March 2024 and so discussed here as a prominent entity of interest to the US policy community. Tracing Dilian's career trajectory helps parse through the complex and convoluted structure of the Intellexa Group.

Dilian, a former commander of the Israel Defense Forces Intelligence Corps' Unit 81,[37] is the founder of several companies that operate or have operated in the spyware market. The first such firm was established in 2010; Circles Solutions Ltd is based in Cyprus and uses Single System 7 vulnerabilities for geolocation with phone numbers as the preferred device identifier, a useful complement to vendors selling spyware targeting mobile phones.[38] In 2014, Dilian sold Circles Solutions Ltd to Francisco Partners, a private equity firm based in the United States. From 2014 to 2019, Francisco Partners also held an "indirect controlling interest" of another spyware vendor, NSO Group.[39, 40, 41] As part of its acquisition, Circles Solutions Ltd became a subsidiary of NSO Group.[42, 43]

Before completing the $130 million sale of Circles to Francisco Partners, Dilian founded WS WiSpear Systems Limited in 2013.[44] WS WiSpear Systems Limited specialized in intercepting target Wi-Fi signals and extracting passwords and communications at long range.[45] In 2018, WS WiSpear Systems Limited acquired the year-old spyware

35 Bill Marczak et al. " Independently Confirming Amnesty Security Lab's Finding of Predator Targeting of U.S. Elected Officials on Twitter/X," *The Citizen Lab*, October 9, 2023, https://citizenlab.ca/2023/10/predator-spyware-targets-us-eu-lawmakers-journalists/.

36 Amnesty International, *Predator Files*.

37 Unit 81 focuses on developing innovative cyber technologies that provide specific functionality for IDF operations. Corin Degani, "An Elite Israeli Intelligence Unit's Soldiers are Sworn to Secrecy – but Tell All on LinkedIn," *Haaretz*, November 18, 2021, https://www.haaretz.com/israel-news/tech-news/2021-11-18/ty-article/.premium/an-israeli-intell-units-soldiers-are-sworn-to-secrecy-but-tell-all-on-linkedin/0000017f-e0e5-d568-ad7f-f3ef63350000. Shuki Sadeh, "A Shady Israeli Intel Genius, His Cyber-Spy Van and Million-Dollar Deals," *Haaretz*, December 31, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000.

38 Thomas Brewster, "A Multimillionaire Surveillance Dealer Steps out of the Shadows...And His $9 Million WhatsApp Hacking Van," *Forbes,* April 5, 2019, https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/?sh=70e4bcfd31b7.

39 Brewster, "A Multimillionaire Surveillance Dealer."

40 NSO Group is an Israel-based spyware vendor that developed the Pegasus spyware suite and has been reported on widely as a focus of a recent EU Parliamentary commission investigation into government abuse of the spyware globally to suppress human rights; see https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/; see https://www.europarl.europa.eu/committees/en/pega/home/highlights.

41 "Operating from the Shadows: Inside NSO Group's Corporate Structure," Amnesty International, May 31, 2021, https://www.amnesty.org/en/documents/doc10/4182/2021/en/.

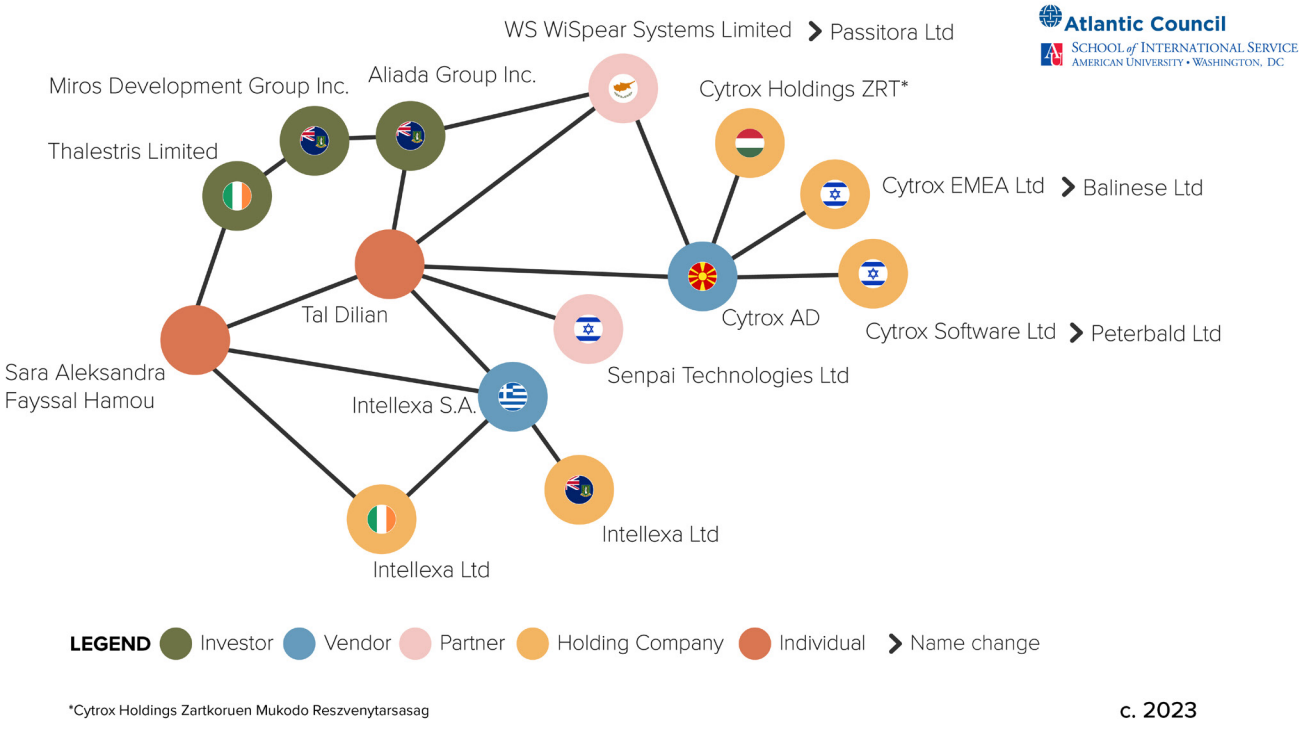
42 "Operating from the Shadows,"https://www.amnesty.org/en/documents/doc10/4182/2021/en/.

43 *European Parliament*, "Report of the Investigation," https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.

44 WS WiSpear Systems, Εφορος Εταιρειών/Registrar of Companies," Accessed March 22, 2024, https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=WS WiSpear Systems Limited&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0. "Operating from the Shadows," Amnesty International.

45 Patrick Howell O'Neil, "Israeli Startup Touting 'the Longest' Range Wi-Fi Spying Tool in the World," *Cyberscoop,* September 21, 2017, https://cyberscoop.com/WS WiSpear Systems Limited-wifi-interception-israel-unit-8200/#:~:text=WS WiSpear Systems Limited%2C%20launched%20in%202016%20by,passwords%20and%20other%20communications%20%E2%80%94%20at%20%E2%80%9C.

Figure 4: Known Companies and Groupings of Intellexa Group



vendor Cytrox AD, based in North Macedonia.[46] Cytrox AD is notable as the original vendor of Predator spyware, the service that would be popularized and sold by Intellexa Group.

In 2018, Dilian began to organize what analysts would later come to term Intellexa Group—to include WS WiSpear Systems Limited (since renamed Passitora Ltd),[47] Cytrox AD, and adding Senpai Technologies Ltd the following year.[48] Senpai Technologies Ltd is an Israel-based company, specializing in open-source intelligence and in analyzing data from phones infected by spyware.[49] This left Intellexa Group with three complimentary offerings for any surveillance-minded government: Cytrox AD's Predator spyware service, WS WiSpear Systems Limited's Wifi-intercept and password-extraction technology, and Senpai Technologies Ltd's data exploitation and open-source research tools.

Two years later, in 2020, Intellexa Group expanded to add Intellexa S.A. (previously known as Intellexa Single Member SA).[50] Intellexa S.A.'s role within this consortium remained unclear until recently, with a corporate registry specifying no more than "computer systems design and related services."[51] In March 2024 however, the US Treasury Department described Intellexa S.A. as the primary channel through which Intellexa Group sells Predator spyware.[52] A global network of investors supports Intellexa, and many companies within Intellexa Group's investor base also

46 *European Parliament,* "Brief for the PEGA Mission."

47 Marczak et al., "Pegasus vs. Predator."

48 *European Parliament,* "Brief for the PEGA Missions"; "Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products," *Amnesty International,* October 6, 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

49 "The Predator Files," Amnesty International, https://www.calcalistech.com/ctech/articles/0,7340,L-3772040,00.html.

50 *European Parliament,* "Brief for the PEGA Mission."

51 "Intellexa S.A.", *dun & bradstreet,* accessed March 22,2024, https://www.dnb.com/business-directory/company-profiles.intellexa_sa.00b9d3be2fdd11150913f55266c391e8.html.

52 US Department of the Treasury, "Treasury Sanctions Members."

have personal connections to Dilian. Aliada Group, based in the British Virgin Islands,[53] has Dilian listed as a shareholder[54] and in 2018 became the majority stakeholder in WS WiSpear Systems Limited,[55] which would go on to acquire Cytrox AD.[56] In 2020, Miros Development Group Inc., based in the British Virgin Islands, purchased Aliada Group.[57] That same year, Miros Development Group Inc. was purchased by Thalestris Limited, a company based in Ireland.[58, 59] The director of Thalestris Limited, Sara Hamou, is Dilian's ex-wife and an offshore specialist.[60]

Intellexa Group distributes corporate ownership through an ecosystem of holding companies. Holding companies are developed to control subsidiaries. Cytrox AD is known to be held by:

- Cytrox Holdings ZRT, based in Hungary
- Cytrox EMEA Ltd (renamed Balinese Ltd in 2019), based in Israel, and,
- Cytrox Software Ltd (renamed Peterbald Ltd in 2019), also based in Israel.[61]

These holding companies may serve to protect the assets and owners within Intellexa Group. Other known limited liability companies bearing the same name of Intellexa also exist in Ireland and the British Virgin Islands as Intellexa Limited. Intellexa S.A. is held by:

- Intellexa Limited based in the British Virgin Islands[62]
- Intellexa Limited based in Ireland[63]

The structure of these holding companies may have been intended to protect assets in the core service provider companies—WS WiSpear Systems Limited, Cytrox AD, and Senpai Technologies Ltd, as well as Dilian and other investors in the Intellexa Group companies.[64, 65]

Intellexa Alliance

Announced in 2019,[66] the Intellexa Alliance was a partnership between the entities that comprise Intellexa Group and those of the Nexa Group.[67] The precise corporate structure of the alliance is murky, and the nature of the relationship remains unknown, although one prominent research outlet has described it as akin to the Star Alliance partnership of airlines.[68] Nexa Group is also used to describe a group of companies that markets a set of products under one name but is not a legal entity itself. It is comprised of Nexa Technologies (France), Nexa Technologies CZ s.r.o. (Czech Republic), Advanced Middle East Systems Fz llc (United

53 *European Parliament,* "Brief for the PEGA Mission."

54 Shuki Sadeh, "A Shady Israeli Intel Genius, His Cyber-Spy Van and Million-Dollar Deals," *Haaretz,* December 31, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000.

55 *European Parliament,* "Brief for the PEGA Mission."

56 *European Parliament,* "Brief for the PEGA Mission."

57 Michalis Hariatis, "The SYRIZA-PASOK Findings on Wiretapping: Both a Scandal and a Cover-Up," *Ieidiseis,* October 10, 2022, https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi.

58 *European Parliament,* "Brief for the PEGA Mission."

59 Colm Keena, "Ireland Being Used by Predator Spyware Group to Avoid Tax, Claims Dutch MEP," *Irish Times,* February 10, 2023, https://www.irishtimes.com/business/economy/2023/02/10/shady-business-ireland-accused-of-facilitating-tax-avoidance-by-spyware-group/; David Kenner, "The Spy, the Lawyer and Their Global Surveillance Empire," *International Consortium of Investigative Journalists,* November 15, 2023, https://www.icij.org/investigations/cyprus-confidential/israeli-predator-spyware-cyprus-offshore-intellexa/.

60 Kenna, "The Spy."

61 "WS WiSpear Systems," Εφορος Εταιρειών/Registrar of Companies, accessed March 22, 2024, https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=WS+WS WISPEAR SYSTEMS LIMITED+SYSTEMS+LIMITED&numbnu=%25&searchtype=optStartMatch&index=1&tname=%25&sc=1; Bill Marczak et al., "Pegasus vs. Predator;" https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=919037&typ=UPLNY; https://www.europarl.europa.eu/RegData/etudes/STUD/2022/738330/IPOL_STU(2022)738330_EN.pdf.

62 "Intellexa Ltd., British Virgin Islands," *Dato Capital,* accessed March 22, 2024, https://www.datocapital.vg/companies/Intellexa-Ltd.html.

63 *Companies Registration Office Ireland*, "Intellexa Limited."

64 Fontinelle, "Holding Company."

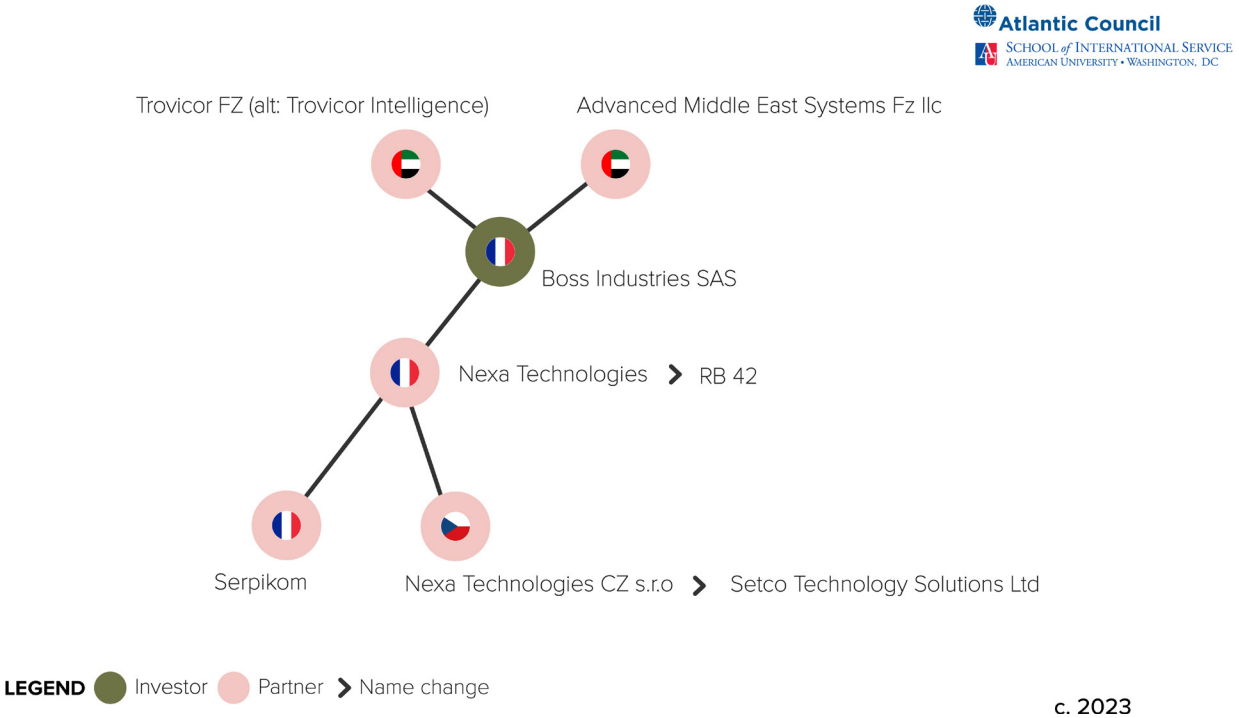
65 US Department of the Treasury, "Treasury Sanctions Members."

66 Nexa Technologies, "Intellexa Alliance," February 16, 2019, https://web.archive.org/web/20200109072024/https:/www.nexatech.fr/intellexa-alliance-press-news.

67 "Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture," *Amnesty International,* June 22,2021, https://www.amnesty.org/en/latest/press-release/2021/06/executives-of-surveillance-companies-amesys-and-nexa-technologies-indicted-for-complicity-in-torture/; Intellexa "The Intellexa Alliance Expands with the Addition of New Members and the Enhancement of Its End-to-End Offering," *Release Wire,* June 20, 2019, http://www.releasewire.com/press-releases/the-intellexa-intelligence-alliance-expands-with-the-addition-of-new-members-and-the-enhancement-of-its-end-to-end-offering-1234811.htm.

68 The Star Alliance in non-spyware space is a partnership of airlines that offer travelers shared benefits for flying within partner airlines; Marczak et al., "Pegasus vs. Predator."

Figure 5: Known Companies and Groupings of Nexa Group



Arab Emirates), Serpikom (France), and Trovicor FZ (United Arab Emirates).

Several key moments provide starting points for analysis of the Nexa Group. In 2012, Nexa Technologies was established as a spin-off of the interception business established by Amesys in France.[69] Founded in 2004, Amesys developed and sold its signature Eagle surveillance technology to the former regime of Muammar Gaddafi in Libya.[70] Eagle expanded traditional techniques by allowing for the surveillance of internet traffic running to an entire country. To implement such a system, Amesys set up "two high-bandwidth 'mirrors'" that copied this traffic into a searchable database for use by government security services.[71] This traffic included voice over Internet Protocol (VoIP) conversations, email, and online chatroom postings.[72] Rather than selecting a few targets to surveil, Eagle allowed the Gaddafi regime to learn about any and all anti-regime activities and discussions taking place over a variety of communications systems.[73]

Bull Group SA (France) bought Amesys in 2010. A year later, the International Federation for Human Rights (FIDH) and the Human Rights League (France) filed a civil party complaint against Amesys and Amesys company executives for "complicity in acts of torture" due to the Libyan government's use of Amesys technologies.[74] However, the court did not approve the opening of an investigation into this matter until 2013, at which point Nexa Technologies had been established to take over Eagle, Amesys' main interception product.

In 2013, two Nexa Group companies were established: Nexa Technologies in France, which took over the development of Eagle surveillance system, and Advanced Middle East Systems in the United Arab Emirates to function as

69 Clairfield International, *Clairfield Annual Outlook 2020,"* January 13, 2020, https://www.clairfield.com/wp-content/uploads/Clairfield-Annual-Outlook-2020.pdf.

70 Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," *The Wall Street Journal,* August 30, 2011, https://www.wsj.com/articles/SB10001424053111904199404576538721260166388.

71 Matthieu Aikins, "Jamming Tripoli: Inside Moammar Gadhafi's Secret Surveillance Network," *Wired*, May 18, 2012, https://www.wired.com/2012/05/ff-libya/.

72 Aikins, "Jamming Tripoli."

73 Aikins, "Jamming Tripoli."

74 International Federation for Human Rights, "Q/A Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies Executives Indicted," June 22, 2021, https://www.fidh.org/en/region/north-africa-middle-east/egypt/q-a-surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa#.

a sales branch for Nexa Technologies products.[75] Nexa Technologies CZ was founded in 2015 as a research and development arm of the company with a particular focus on cryptography.[76] Nexa Technologies built upon Eagle to produce and sell its successor product, Cerebro, to governments in Egypt, Kazakhstan, Qatar, Singapore, and the United Arab Emirates.[77] In 2019, Boss Industries, the parent company of Nexa Group, acquired Trovicor fz/Trovicor Intelligence, a competing company in the interception technology space. Like its predecessor Amesys, in 2021, Nexa Technologies found itself under indictment for "complicity in acts of torture and of enforced disappearances" based on the Egyptian government's use of Cerebro technologies against its citizens.[78]

Nexa Group companies underwent several name changes over the years. As early as 2019, Boss Industries likely held ownership of Nexa Group companies including Nexa Technologies (France), Nexa Technologies CZ, Advanced Middle East Systems (United Arab Emirates), Trovicor fz/Trovicor Intelligence (United Arab Emirates), and Serpikom (France).[79] In 2021, ChapsVision acquired Nexa Technologies France.[80] The government-facing branch of ChapsVision now purports to build "a sovereign cyber intelligence and cyber security solution, dedicated to the defence, intelligence and security markets".[81] As of 2022, Nexa Technologies CZ operates under the name Setco Technology Solutions, and as of 2023, Nexa Technologies (France) operates under the name RB 42.[82, 83]

Nexa Technologies' integrated hardware-software surveillance product might well have complemented the Intellexa Group companies' spyware and related service offerings. Nexa's Cerebro allowed for the passive surveillance of entire populations. Cerebro collects massive amounts of communications data to identify potential targets for enhanced surveillance scrutiny. Once Cerebro identifies a target, Intellexa could deploy Predator spyware to infect that individual's device to collect more intimate data.

Intellexa Consortium - Interaction with Suppliers and Customers

Some spyware vendors rely primarily on procuring their vulnerabilities and exploits from third-party suppliers,[84] while others, like NSO Group, balance procuring these tools from the market with their own in-house research and development.[85] Intellexa Group companies appear to source exploits to support the Predator spyware with enough speed to maintain an eight-figure price point for the product, suggesting both in-house and third-party suppliers for exploits and vulnerability information.[86 87] Suppliers from which the Intellexa Group purchases vulnerabilities and exploits is not publicly available.

The Intellexa Consortium has faced scrutiny for where and to whom they have sold their wares. In 2007, a known member of the Intellexa Alliance, Nexa Technologies (France)—operating at the time as Amesys—sold its surveillance hardware to Libya. In 2011 and again in 2014, the International Federation for Human Rights and the Human Rights League filed complaints against Nexa Technologies for complicity in acts of torture from the sale of this technology.[88, 89]

75 Clairfield International, "Project <<Aspen>> Expert in Homeland Security Solutions,"Clairfield International. September 2016. https://s3.documentcloud.org/documents/21116576/project-cerebro-nexa-technologies.pdf.

76 Clairfield, "Project Aspen."

77 Sven Becker et al., "European Spyware Consortium Supplied Despots and Dictators," *Spiegel International,* May 10, 2023, https://www.spiegel.de/international/business/the-predator-files-european-spyware-consortium-supplied-despots-and-dictators-a-2fd8043f-c5c1-4b05-b5a6-e8f8b9949978.

78 International Federation for Human Rights, "Surveillance and Torture."

79 "The Predator Files," Amnesty International.

80 "Raising the Bar: A Selection of M&A Deals," Eversheds Sutherland, Accessed March 22, 2024. https://www.es-archive.com/documents/global/czech-republic/cz/Tombstone%20M&A_CR_SR.pdf.

81 "ChapVision Cybergov", accessed March 22, 2024, https://www.chapsvision-cybergov.com/.

82 "Setco Technology Solutions s.r.o.," Verejny restrik (obchodni rejstrik)/Public Register (Commercial Register), Accessed March 22, 2024, https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=919037&typ=UPLNY

83 "The Predator Files," Amnesty International.

84 "Hacking Team: a zero-day market case study," Vlad Tsyrklevich, (personal website), July 22, 2015, https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/.

85 Winnona DeSombre et. al "Countering Cyber Proliferation."

86 Victor Ventura, "Intellexa and Cytrox AD: From Fixer-Upper to Intel Agency-Grade Spyware," *Talos,* December 21, 2023, https://blog.talosintelligence.com/intellexa-and-Cytrox AD-intel-agency-grade-spyware/.

87 "Read the Intellexa Pitch," *The New York Times*.

88 International Federation for Human Rights, "FIDH and LDH File a Complaint Concerning the Responsibility of the Company AMESYS in Relation to Acts of Torture," October 19, 2011, https://www.fidh.org/en/region/north-africa-middle-east/libya/FIDHand-LDH-file-a-complaint.

89 International Federation for Human Rights, "Q/A Surveillance."

In 2022, the *Guardian* newspaper revealed that Predator spyware had been used to monitor individuals across Greek politics through the Greek intelligence service.[90] Most recently, Intellexa Group companies have been accused of selling Predator to a customer aligned with government interests in Vietnam.[91] In 2021, the civil society group Citizen Lab also reported "likely customers" of Predator in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia.[92]

Recent Policy Action on Spyware

In 2022, in response to the investigative findings of the Pegasus Project, an international investigative journalism initiative, the European Parliament set up the PEGA Committee to investigate the misuse of surveillance spyware including the NSO Group's Pegasus and similar spyware services.[93] The committee concluded that European Union governments abused spyware services, lacked necessary safeguards to prevent misuse, and in one jurisdiction the government even facilitated the heedless export of spyware technologies to authoritarian regimes.[94] Despite the committee's recommendations, the EU has not adopted any legislation as a bloc to curb the development or sale of spyware. In March 2023, the United States first proposed to block the US government agencies' operational use of "commercial spyware." Under Executive Order 14093, the Biden administration prohibited the operational use of commercial spyware that presents a significant threat to national security.[95] Four months later, the US Department of Commerce added four Intellexa Group companies to its Entity List alongside other spyware vendors NSO Group and Candiru, to curb these firms' ability to obtain commodities, software, and technology needed to develop spyware surveillance tools.[96] The move targeted four entities: Intellexa S.A., Cytrox AD Holdings ZRT, Intellexa Limited (Ireland), and Cytrox AD (North Macedonia) because they were "trafficking cyber exploits … used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide."[97]

In 2024, the US Department of Treasury Office of Foreign Assets Control levied sanctions against several of the entities listed in the 2023 Commerce action, while adding three more.[98] Ultimately Treasury sanctioned Tal Dilian, Sara Hamou, Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings Crt, and Thalestris Limited.[99] So far, US actions have not included at least five additional entities within the Intellexa Group, Balinese Ltd (formerly Cytrox AD Software Ltd), Peterbald Ltd (formerly Cytrox AD EMEA Ltd), Passitora Ltd (formerly WS WiSpear Systems Limited), and Senpai Technologies Ltd, as well as the British Virgin Islands-domiciled Intellexa Limited.

90 Helena Smith, "Greek 'Watergate' Phone-Tapping Scandal Puts Added Pressure on PM," *The Guardian*, August 28, 2022, https://www.theguardian.com/world/2022/aug/28/greek-watergate-phone-tapping-scandal-threatens-to-topple-pm.

91 "The Predator Files," Amnesty International.

92 Marczak et al., "Pegasus vs. Predator."

93 "Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Sse of Pegasus and Equivalent Surveillance Spyware," *European Parliament,* May 22, 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.

94 *European Commission,* "Report on the Investigation."

95 The White House, "Fact Sheet: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware That Poses Risks to National Security," 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/.

96 US Department of Commerce, "Commerce Adds Four Entities to Entity List for Trafficking in Cyber Exploits," July 18, 2023, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3297-2023-07-18-bis-press-package-spyware-document/file.

97 US Department of Commerce, "Commerce Adds Four."

98 This sanction designation freezes all assets held in the United States and prohibits these individuals and entities from conducting business within the United States. Furthermore, if a financial institution continues to do business with these designated entities and individuals, it may be subject to sanctions or enforcement actions. Finally, if a sanctioned individual or entity owns 50 percent or more of a company not listed, those firms are also subject to sanctions.

99 US Department of the Treasury, "Treasury Sanctions Members."

Takeaways for Policy and Research

Each member company of the Intellexa Consortium sells spyware or ancillary surveillance support capabilities. The Intellexa Group offers a vertical integration of spyware targeting and delivery as well as information exploitation services. The Intellexa Alliance extends that integration to cover several major European jurisdictions. By bringing talent and complimentary services under an interlinked set of corporate partners, the Intellexa Consortium aggregates behaviors observed from other spyware vendors into a tighter, more robust cluster of entities.

This expansiveness of firms across various geographies allows the Intellexa Consortium to exploit jurisdictional arbitrage that can result in different regulatory treatment of the same transaction in different legal systems. Just like in the case of financial arbitrage, high costs are an impediment to arbitrage. In policy for spyware, high transaction costs could act as hindrance to leave a jurisdiction and high entry costs into a more favorable jurisdiction, thus inhibiting this activity in practice. Policymakers could achieve this by requiring more detailed disclosure of where companies intend to relocate when exiting a jurisdiction and their business purpose as well as strengthening business incorporation rules and laws to include more robust investigation of intended business activities of companies (and their beneficial owners, such as a recent change in US reporting rules).[100] Media reporting about the Intellexa Consortium often reduces this sprawling group of companies to a single entity, which makes it difficult to identify the operating jurisdiction of that firm. Policymakers should also consider providing universal jurisdiction for cases of spyware with other like-minded states. Cyprus, the Czech Republic, France, Greece, Hungary, Ireland, Israel, and US[101] already provide for universal jurisdiction over certain kinds of crimes, a fruitful existing coalition to pursue such a change.

Virtually no information exists to explain the business consequences of Intellexa Alliance "membership." Policymakers cannot make sense of how to target parts or all of the alliance without clearly understanding the constraints of this relationship.

Efforts to improve transparency in, and limit the harms of, the spyware market are hobbled if they focus solely on transactions or individual vendors. The rich ties of influence over participants in this market are in their financial and organizational dependencies with others. Policymakers must consider a multipronged approach that incorporates action for not only vendors themselves, but also key subsidiaries, investors, suppliers, and individuals that make up this market. Ably demonstrated by the Intellexa Consortium, the ebb and flow of corporate relationships, constant name changes, and confusing business structures, not only makes it difficult to track what is happening behind the veil with a vendor, but makes policy strictly chasing vendors neglect other pieces of this puzzle.

Enhancing the transparency of this market would provide more accurate and timely information to policymakers. Proposals for governments to create know-your-vendor requirements for all those from whom they acquire spyware or related services would substantially benefit policymakers' visibility into this market and these relationships. Better information about spyware vendor's business structures would help drive precise regulatory activity and allow for improved awareness of jurisdictions providing a ready home for investors, or vendors, associated with particular harms.

This transparency would help realize more effective targets of enforcement as well. Vendors change, but individuals often move between them. Transparency about ownership will assist policymakers in regulating individuals associated with spyware vendors, their subsidiaries, as well as investors. The Intellexa Consortium highlights a vital detail in this picture, where individuals who cultivate businesses around spyware will be repeat players in the market. Tal Dilian was founder of Circles Solutions (now under the NSO Group umbrella) and WS WiSpear Systems Limited (the majority stakeholder in Cytrox AD), along with creating the Intellexa Group. Enhancing transparency in this market will help policymakers find and fix on critical individuals within this market rather than only playing whack a mole with corporate registries.

A final potential benefit of this improved transparency is the prospect for efficient regulation of investors. While vendors' jurisdictions might sometimes be outside the reach of proactive states, publicly known investors in spyware companies appear, at present, to be concentrated in geographies with government interest in intervention against

100 "New Report: US is catching up with beneficial ownership," *Thomas Reuters,* January 24, 2023, https://www.thomsonreuters.com/en-us/posts/corporates/beneficial-ownership-report-2024/.

101 "Universal Jurisdiction: A Preliminary Survey of Legislation Around the World – 2012 Update," Amnesty International, October 09, 2012, https://www.amnesty.org/en/documents/ior53/019/2012/en/.

the spyware market, notably the US and UK. For example, while the Intellexa Consortium operates largely within the European Union as a vendor, several of its holding companies and investors are based in the continental United States and the British Virgin Islands. More widely, a 2021 report from Amnesty International found that out of the 50 largest venture capital firms and three start up accelerators worldwide, only one had any sort of due diligence processes for human rights.[102]

The case of the Intellexa Consortium is curious for the internal complexity of these firms' relationships and the potential these business relationships hold for policymakers, researchers, and advocates working to limit the harms of the spyware market. The case is an example of the value that a market perspective can hold as well as the analytic challenges posed by contemporary research into these vendors and their activities. The prospects for policy in this domain are bright and for the first time in more than a decade hold the potential for material change in the shape and impact of the spyware market. We remain hopeful that potential will be realized.

Acknowledgements

Thank you to more than two dozen researchers and analysts who shared their time, expertise, and feedback in the development of this project. Credit is owed to Jen Roberts, for the initial design of many of these graphics, and to Winnona DeSombre Bernsen for her tireless analysis and support throughout the development of this paper. Major thanks to Sopo Gelava, Jean le Roux, and Nancy Messieh who did foundational work on this dataset and its visualization. Thank you for peer review of this paper to Graham Brookie, Winnona DeSombre Bernsen, Kimberly Donovan, Maia Hamin, Kirsten Hazelrig, Sarah McKune, Stewart Scott, and several others who shall remain anonymous. Finally, the authors wish to acknowledge the often-thankless work of those journalists, researchers, and a small community of government analysts and policymakers who have sought to understand this market and its impact on people around the world. There is little in this or any other art which springs forth entirely original and we owe a debt of gratitude to their efforts. The team gratefully acknowledges support for this work from Microsoft and the UK National Cyber Security Centre.

102 "Risky Business: How Leading venture Capital Firms Ignore Human Rights when Investing in Technology," *Amnesty International,* July 30, 2021, https://www.amnesty.org/en/documents/doc10/4449/2021/en/.

About the Authors

Jen Roberts is an Assistant Director with the Atlantic Council's Cyber Statecraft Initiative. She primarily works on CSI's Proliferation of Offensive Cyber Capabilities and Combating Cybercrime work. Jen also helps support the Cyber 9/12 Strategy Challenge and is passionate about how the United States with its allies and partners, especially in the Indo-Pacific, can cooperate in the cyber domain. Jen holds an MA in International Relations and Economics from Johns Hopkins University's School of Advanced International Studies (SAIS) where she concentrated in Strategic Studies. She also attained her BA in International Studies from American University's School of International Service.

Trey Herr is assistant professor of Global Security and Policy at American University's School of International Service and Senior Director of the Atlantic Council's Cyber Statecraft Initiative. At the Council, the CSI team works at the intersection of cybersecurity and geopolitics across conflict, cloud computing, supply chain policy, and more. At American, Trey's work focuses on complex interactions between states and non-state groups, especially firms, in cyberspace. Previously, he was a senior security strategist with Microsoft handling cybersecurity policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Emma Taylor is a Research Assistant with the School of International Service and a highly interdisciplinary professional pursuing an M.S. in Computer Science and Cybersecurity with previous experience in the technology industry.

Nitansha Bansal is an Assistant Director with the Atlantic Council's Cyber Statecraft Initiative. Prior to joining the Council, Bansal worked with the Government and Public Affairs team of Open Source Elections Technology Institute (OSET) where she created visual dashboard for enhancing transparency in American elections. Previously, she worked as a Research Associate with Takshashila Institution, a think tank in India at the intersection of space and cybersecurity policy, and advised Members of Parliament in India on multiple legislative, economic and policy issues. Bansal holds a Masters in Public Administration from Columbia University's School of International and Public Affairs. Her course of study was concentrated on cyber espionage, cybersecurity and business risk, mis/disinformation, social media policy, deepfake, and trust and safety. Originally from New Delhi, India, she speaks Hindi and Rajasthani.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Alain Bejjani
Colleen Bell
Sarah E. Beshar
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ankit N. Desai
Dario Deste
*Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Stuart E. Eizenstat
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Francesco G. Valente
Melanne Verveer
Tyson Voelkel
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of March 27, 2024

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.

1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org