Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

#ACcyber

ISSUE BRIEF

NOVEMBER 2021

Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets

WINNONA DESOMBRE,
LARS GJESVIK,
AND JOHANN OLE WILLERS

EXECUTIVE SUMMARY

State cyber capabilities are increasingly abiding by the "pay-to-play" model—both US/NATO allies and adversaries can purchase interception and intrusion technologies from private firms for intelligence and surveillance purposes. NSO Group has repeatedly made headlines in 2021 for targeting government entities in cyberspace, but there are many more companies selling similar products that are just as detrimental. These vendors are increasingly looking to foreign governments to hawk their wares, and policymakers have yet to sufficiently recognize or respond to this emerging problem. Any cyber capabilities sold to foreign governments carry a risk: these capabilities could be used against individuals and organizations in allied countries, or even in one's home country.

Because much of this industry operates in the shadows, research into the industry in aggregate is rare. This paper analyzes active providers of interception/intrusion capabilities within the international surveillance market, cataloguing firms that have attended both ISSWorld (i.e., the Wiretapper's Ball) and international arms fairs over the last twenty years.[1] This dataset mostly focuses on Western firms and includes little on Chinese firms, due to historical under-attendance of Chinese firms at ISSWorld. However, the overarching nature of this work will help policymakers better understand the market at large, as well as the primary arms fairs at which these players operate. This paper identifies companies explicitly marketing interception/intrusion technology at arms fairs, and answers a series of questions, including: what companies are marketing interception/intrusion capabilities outside their headquartered region; which arms fairs and countries host a majority of these firms; and what companies market interception/intrusion capabilities to US and NATO adversaries?

The resulting dataset shows that there are **multiple firms headquartered in Europe and the Middle East** that the authors assess, with high confidence, **are mar-**

keting cyber interception/intrusion capabilities to US/NATO adversaries. They assume that companies offering interception/intrusion capabilities pose the greatest risk, both by bolstering oppressive regimes and by the proliferation of strategic capabilities.[2] Many such firms congregate at Milipol France, Security & Policing UK, and other arms fairs in the UK, Germany, Singapore, Israel, and Qatar.

The authors found that 75 percent of companies likely selling interception/intrusion technologies have marketed these capabilities to governments outside their home continent. Five irresponsible proliferators—BTT, Cellebrite, Micro Systemation AB, Verint, and Vastech—have marketed their capabilities to US/NATO adversaries in the last ten years.[3]

This paper categorizes these companies as potentially irresponsible proliferators because of their willingness to market outside their continents to nonallied governments of the United States and NATO—specifically, Russia and China.[4] By marketing to these parties, these firms signal that they are willing to accept or ignore the risk that their products will bolster the capabilities of client governments that might wish to threaten US/NATO national security or harm marginalized populations. This is especially the case when the client government is a direct US or NATO adversary.

This globalizing shift is important for two reasons. First, it indicates a widening pattern of proliferation of cyber capabilities across the globe. Second, many firms in the surveillance and offensive cyber capabilities markets have long argued for the legitimacy of their business model by pointing to the perceived legitimacy of their customers; yet, their marketing strategies contradict this argument. As the recent indictment of several former US intelligence personnel working for the United Arab Emirates (UAE) confirms, capabilities originally focusing on one target set may be expanded for other intelligence uses.[5] When these firms begin to sell their wares to both NATO members and adversaries, it should provoke national security concerns for all customers.

This paper profiles these important trends for their practical security impacts, and to enable further research into this topic. The authors suggest that the United States and NATO

- create know-your-customer (KYC) policies with companies operating in this space;
- work with arms fairs to limit irresponsible proliferators' attendance at these events;
- tighten export-control loopholes; and
- name and shame both irresponsible vendors and customers.

The authors encourage policymakers to focus their efforts to rein in companies that sell these capabilities directly to adversaries, or those willing to ignore the risk that their capabilities may be misused. The dataset presented below is open for use by others who might similarly seek to bring some measure of light to an industry that remains so insistently in the dark.

INTRODUCTION

Offensive cyber capabilities are becoming increasingly privatized.[6] Governments no longer need to devote significant resources to develop offensive cyber capabilities in house—in fact, almost any government can buy capabilities to accomplish a range of national security objectives, including the surveillance of domestic groups, cyber defense, foreign-intelligence collection, and the bolstering of traditional military capabilities.[7] What used to be a "nobody but us" system—in which cyber capabilities were difficult to develop and the prerogative of a limited number of states—has evolved into a "pay-to-play" model in which any government, adversary or ally, can gain access to offensive cyber capabilities if it can hire the right firm.[8]

While offensive cyber capabilities are helpful for law enforcement and border protection, the dual-use nature of many of these capabilities provides opportunity for malicious employment as well, especially when the capabilities are sold to authoritarian actors.[9] Examples abound. Executives of French-owned spyware vendor Amesys/Nexa were indicted for their role in supplying the Egyptian and Libyan regimes with surveillance and intrusion capabilities during the Arab Spring.[10] Israeli NSO Group/Q Cyber has achieved much unwanted notoriety for its Pegasus spyware, which provides authoritarian governments around the world the capability to spy on journalists, political opposition, and activists.[11] Beyond human-rights violations, cyber capabilities sold to even regional partners of the United States and NATO may be used against the United States and NATO in the future. Emirati firm DarkMatter took over programs created by US-based Cyberpoint with help from former US intelligence employees and used those capabilities, in part, to monitor US citizens.[12]

These cases and others highlight how private companies, especially those offering intrusion or "lawful" interception products, have become vital vectors of proliferation of offensive cyber capabilities (OCC).[13] As the number of controversial incidents of privately developed cyber capabilities is increasing, calls to rein in the operations of this market are growing.[14] While some argue for an arms-control treaty for cyberspace, regulating cyber capabilities themselves is largely ineffective.[15] Instead, shaping the behaviors of companies proliferating cyber capabilities, and limiting their activities where they conflict with national security priorities, should be the top priority.[16]

However, this means first identifying those companies acting as irresponsible proliferators. Are there conferences at which these organizations tend to congregate? Which companies are marketing their wares internationally to countries that may use these capabilities against the United States, NATO, and their allies?

The surveillance industry is multifaceted, covering a range of products and use cases. The authors assume that companies offering interception or intrusion capabilities pose the greatest risk, as suggested by the wide range of cases of misuse involving companies like NSO Group, Cellebrite, DarkMatter,

and other similar firms.[17] The authors have labeled companies marketing these capabilities outside their country or continent, especially to US/NATO adversaries, as irresponsible proliferators. By marketing to these parties, these firms signal that they are willing to accept or ignore the risk that their products may bolster the capabilities of authoritarian and/or adversary governments, which may use their products to target vulnerable populations within their country or conduct foreign espionage more effectively.

The offensive cyber industry remains poorly understood by the public, and current knowledge is based on case studies of individual companies. Little systemic knowledge about the industry exists, largely due to the opaque nature of the surveillance industry. As a result, differentiating legitimately operating companies from those that enable human-rights violations is difficult.[18]

To address this issue, this paper focuses on companies that are marketing interception/intrusion capabilities (e.g., mobile forensics, "lawful interception services," non-passive communication interception/monitoring, spyware, surveillance capabilities), and also *explicitly marketing* their capabilities at foreign arms fairs. These companies are often unambiguously operating on the offensive side of the market, and present a compelling target for regulatory action.

This paper identifies companies explicitly marketing interception/intrusion technology at arms fairs, and interrogates this new dataset to answer the following questions.

1. What firms are marketing interception/intrusion capabilities at arms fairs? How has this evolved over time?
2. What companies are marketing interception/intrusion capabilities outside their headquartered region?
3. Which arms fairs (and which arms fair host countries) host a majority of these firms?
4. Critically, what companies are marketing interception/intrusion capabilities to US and NATO adversaries?

The answers to these questions will allow policymakers to better understand the market at large by enumerating players selling interception/intrusion capabilities, as well as the primary arms fairs at which these players operate. These answers also underline the overwhelming importance of addressing the shape and permissive existence of the market, not just the behavior of individual firms, as it extends globally and reaches into an increasing number of countries, including those that might leverage its capabilities counter to the interests of the United States and NATO. The proliferation of cyber capabilities in the hands of irresponsible corporate actors presents an urgent challenge to the policymaking community.

METHODOLOGY, ASSUMPTIONS, AND LIMITATIONS

To answer the stated questions, this paper compares the Omega Foundation's Arms Fair database of more than one hundred and seven thousand exhibitors to historical speaker and sponsor organizations at ISSWorld, to create a database of companies featured at both events.[19]

Debuting in the early 2000s, ISSWorld is the premier dedicated trade show for lawful interception and intrusion products.[20] The authors catalogued sixty-four unique conference brochures via The Wayback Machine and other publicly available sources. For each conference, they gathered publicly available information about sponsors and presenting companies, the year and location of the conference, and the title of presentations. These brochures encompass seven hundred and seventy-seven unique ISSWorld speaker and sponsor organizations across the Middle Eastern, Latin American, European, Southeast Asian, and North American conference series between 2003 and 2020.

In the subsequent analysis, the paper compares the seven hundred and seventy-seven organizations at ISSWorld against the 107,542 unique exhibitors at arms and law-enforcement fairs from the Omega Foundation's Arms Fair Dataset.[21] Using a simple program to identify names present in both datasets, the authors identified two hundred and twenty-four companies.[22] They manually cleaned the matches to ensure the robustness of the dataset and added contextual information about the vendors. All matches were categorized according to the confidence level (high/medium/low) that a given vendor attended an arms fair to promote interception and/or intrusion technologies.

The dataset also utilizes the resulting high/medium/low classification to identify the arms fairs with the most "high confidence" companies (i.e., in any given arms fair, which companies are likely to be attending primarily to market interception/intrusion capabilities?). To ensure the robustness of this coding (and confidence levels), two of the authors independently checked and compared results.

This methodology resulted in the following matches. The full list of companies is in the Appendix, and the full dataset with classifications can be found there.[23]

Number of unique arms-fairs exhibitors: 107,542
Number of unique ISSWorld sponsor/speaker companies: 777
Number of matches: 224

In other words, around three in ten companies in the dataset that have sponsored an ISSWorld conference or sent individuals to speak at ISSWorld have also been an exhibitor at an arms fair in the last twenty years.

The dataset presented here **does not** cover transactions. The authors assume that a company going to an arms fair or ISSWorld as an exhibitor (or sponsoring or sending speakers to ISSWorld) reveals a company's willingness to enter the surveillance marketplace in that geographical region.

This paper is not an exhaustive survey of the intrusion/interception capability industry, but rather profiles an important nexus between this industry and traditional arms brokers. There are likely missing players from this spreadsheet that do not frequent the arms fairs/ISSWorld conferences in the dataset, or that care more about their operational security (OPSEC) than about marketing at these two types of events, introducing a bias toward larger, globalized, and more public firms.

Matches can also have ambiguous results, especially if a company has a generic name (such as "Nice," "Pegasus," etc.). Where the authors were unable to determine whether the ISSWorld exhibitor was the same as the arms-fair exhibitor in a match, the firm was not included in the final dataset.[24] In these, and other, areas the authors encourage further exploration and additions to this dataset.

The confidence classifications (high/medium/low) and firm headquarters locations used here are also a composite of open-source research and feedback from trusted industry partners. All high-confidence companies have been confirmed by multiple sources, while firms at other confidence rankings might see some discrepancy. In all cases, coding is conservative, and disagreement among sources or ambiguity is reflected in lower confidence levels.

Finally, the software used to generate matches searched only in English, and so missed Cyrillic or Chinese characters. On top of this, ISSWorld is historically attended by far more Western firms than Chinese firms. Because of these two factors, and this paper's conservative confidence classifications, the authors believe that the dataset woefully underreports the presence of Chinese companies in this space. China has made surveillance capabilities a key part of its Digital Silk Road initiative, providing training and surveillance services to interested partner countries.[25] However, Chinese companies are not required to have an English name, and translations of Chinese names into English can be inconsistent.[26] Thus, the software for this dataset likely missed a few Chinese companies due to inconsistent translations. Chinese companies Huawei and ZTE do show up in the dataset, and they have track records of selling surveillance capabilities to telecommunications firms in Uganda and Iran, respectively.[27] However, because the authors cannot say with high confidence that these firms were marketing these capabilities at the arms fairs they attended, the authors left them out of other analysis. Their attendance at arms fairs and ISSWorld can be found in the data visualization in Appendix A.

These factors, when taken together, suggest that there are likely far more companies operating in this market than the two hundred and twenty-four identified.

MAIN FINDINGS

1. What firms are marketing interception/intrusion capabilities at arms fairs?

Number of matches: 224		
High confidence: 59	Medium confidence: 22	Low confidence: 143

Of the **two hundred and twenty-four organizations total** (full list in the Appendix), fifty-nine are high-confidence matches. The authors assess these companies are highly likely to market interception/intrusion technologies at any arms fair they attend. Some of the companies (like Croatia's Pro4Sec and India's ClearTrail) advertise lawful interception services on their websites for military, law-enforcement, and intelligence-agency clients.[28] Others (like Italy's Area s.p.a and Germany's Wolf Intelligence) have vague websites or no websites at all, but have been called out by news media for selling interception/intrusion tools.[29]

The twenty-two medium-confidence companies are somewhat likely to promote interception/intrusion technology at an arms fair. These twenty-two companies all offer interception/intrusion technology, but it is not their primary product or service. For example, companies like France's Deveryware offer forensics solutions, geolocation, and data analytics, and may be marketing any one (or all three) of these services at any given time.[30]

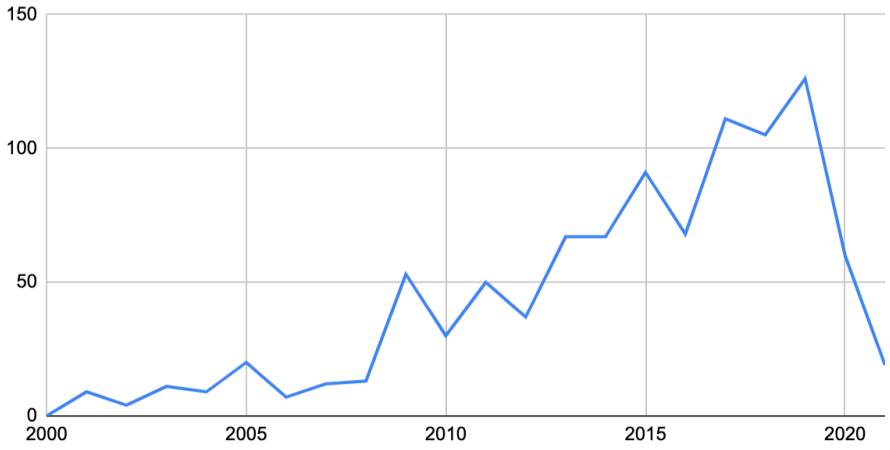
The one hundred and forty-three low-confidence companies are far less likely to promote interception/intrusion technologies at an arms fair. Some of these companies include formal defense contractors (like BAE and Raytheon) that offer both interception/intrusion capabilities and traditional military or law-enforcement equipment. There are also different companies on the list, including telecommunications firms (like China's Huawei and ZTE) and smaller firms selling defensive and/or tangential cybersecurity products. The authors exclude these organizations in some parts of the piece to focus on high/medium-confidence companies, but the fact that these organizations have been to both ISSWorld and an arms fair is worth further analysis in future pieces.

a. How has this evolved over time?

Of the companies that have sent representatives to ISSWorld, the subset that has also attended arms fairs as exhibitors is largely **increasing over time**, likely due to the increasing number of surveillance firms entering the market. The two hundred and twenty-four total matches consist of 0.21 percent of the overall arms-fair exhibitors, but 28.96 percent of the ISSWorld speaker/sponsor organizations. In other words, almost **three in ten** companies from the dataset that have sponsored or sent individuals to speak at an ISSWorld conference have also been an exhibitor at an arms fair in the last twenty years.

Figure 1.

Number of ISSWorld Matches by Arms Fair Attendance in a Given Year



As the heatmap below shows, most of these companies have attended either an arms fair or ISSWorld between the years 2009–2020, likely because many of these companies were not founded or not offering offensive cyber capabilities prior to 2009.[31] The steep drop in 2020–2021 is due to lack of conference data, rather than lack of players. There does not seem to be a preference toward one type of conference or the other within the industry. This is likely because, while surveillance companies have expanded into the military space, ISSWorld has also significantly expanded its focus to invite military and intelligence organizations.

Figure 2.

Arms Fair and ISSWorld Attendance Across High Confidence Companies

https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#attendanceovertime

Figure 2. cont.

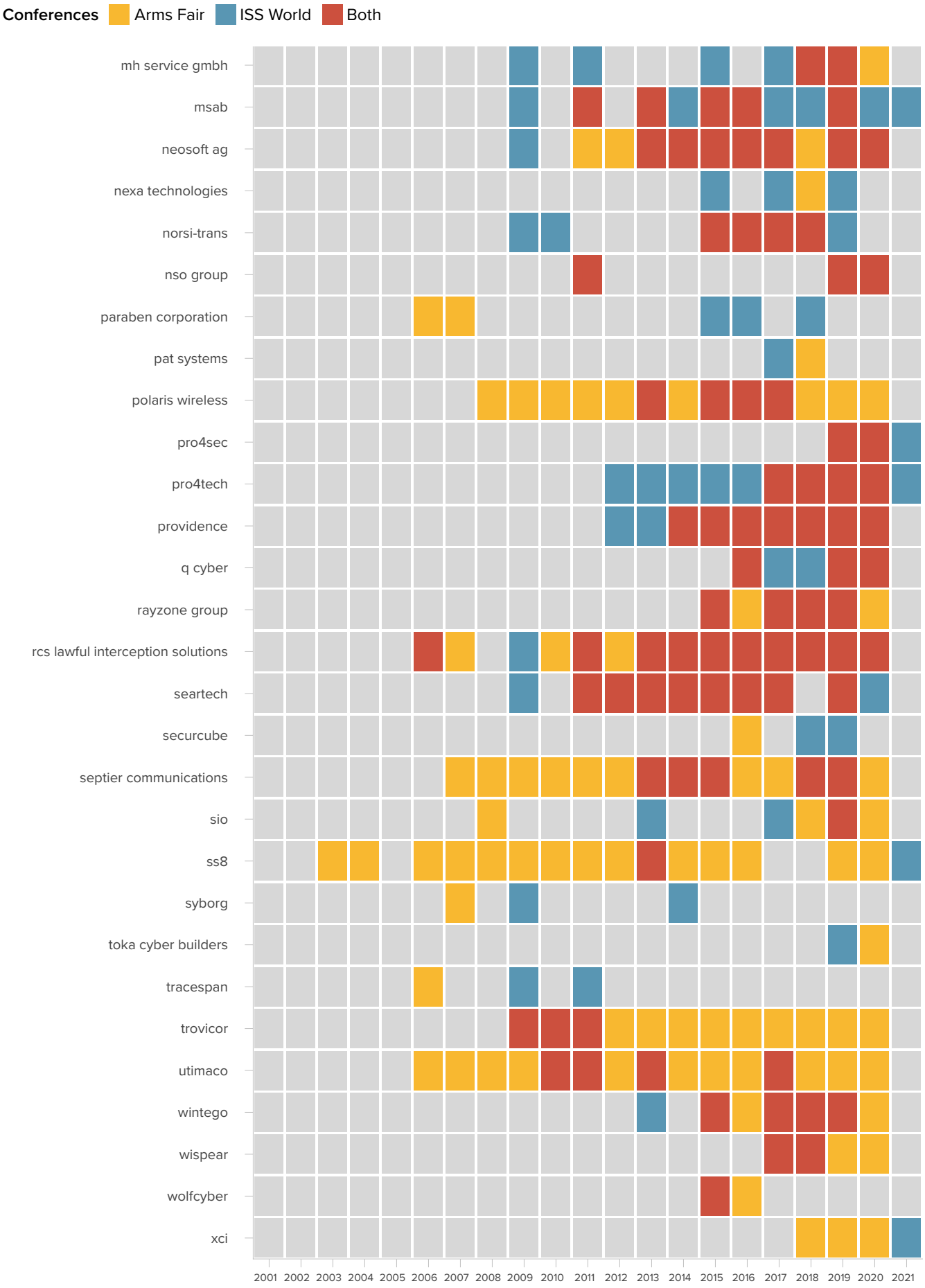


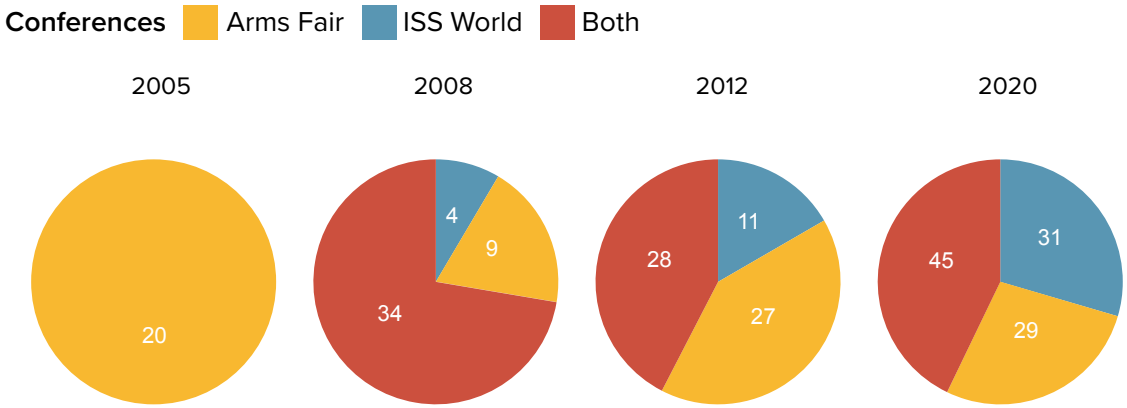
Figure 2. cont.

Arms Fair and ISSWorld Attendance Across Medium Confidence Companies

In fact, the number of companies to attend both an ISSWorld conference and an arms fair in a single year has stayed fairly consistent, relative to the number of total firms, over the last ten years. Between 2009 and 2020, between 20–40 percent of companies, on average, had attended both an arms fair and an ISSWorld conference in the same year.

Figure 3.

Arms Fair and ISSWorld Attendance by Year Across All Companies



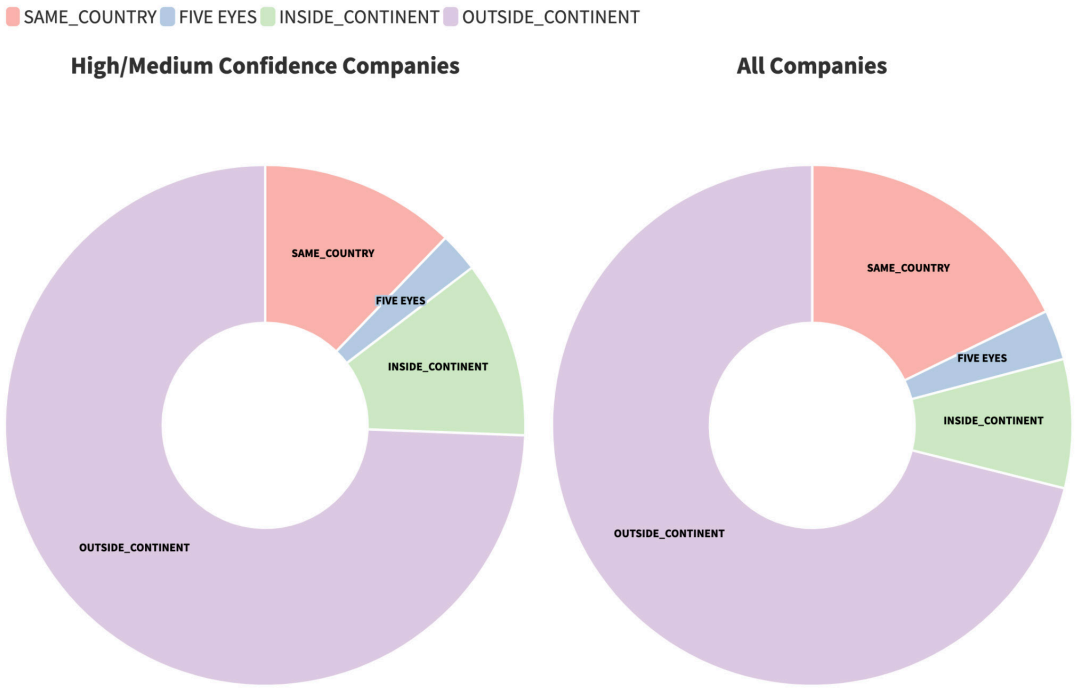
https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#attendancebyyear

2. What companies are marketing interception/intrusion capabilities outside their headquartered region?

This question focuses only on the high/medium-confidence companies, as the authors cannot assess whether the low-confidence companies have been marketing these capabilities at arms fairs with enough certainty. For the high/medium-confidence companies, the data show a general willingness to market interception/intrusion capabilities internationally, even to foreign countries that do not have established intelligence relationships or alliances with the company's home country.

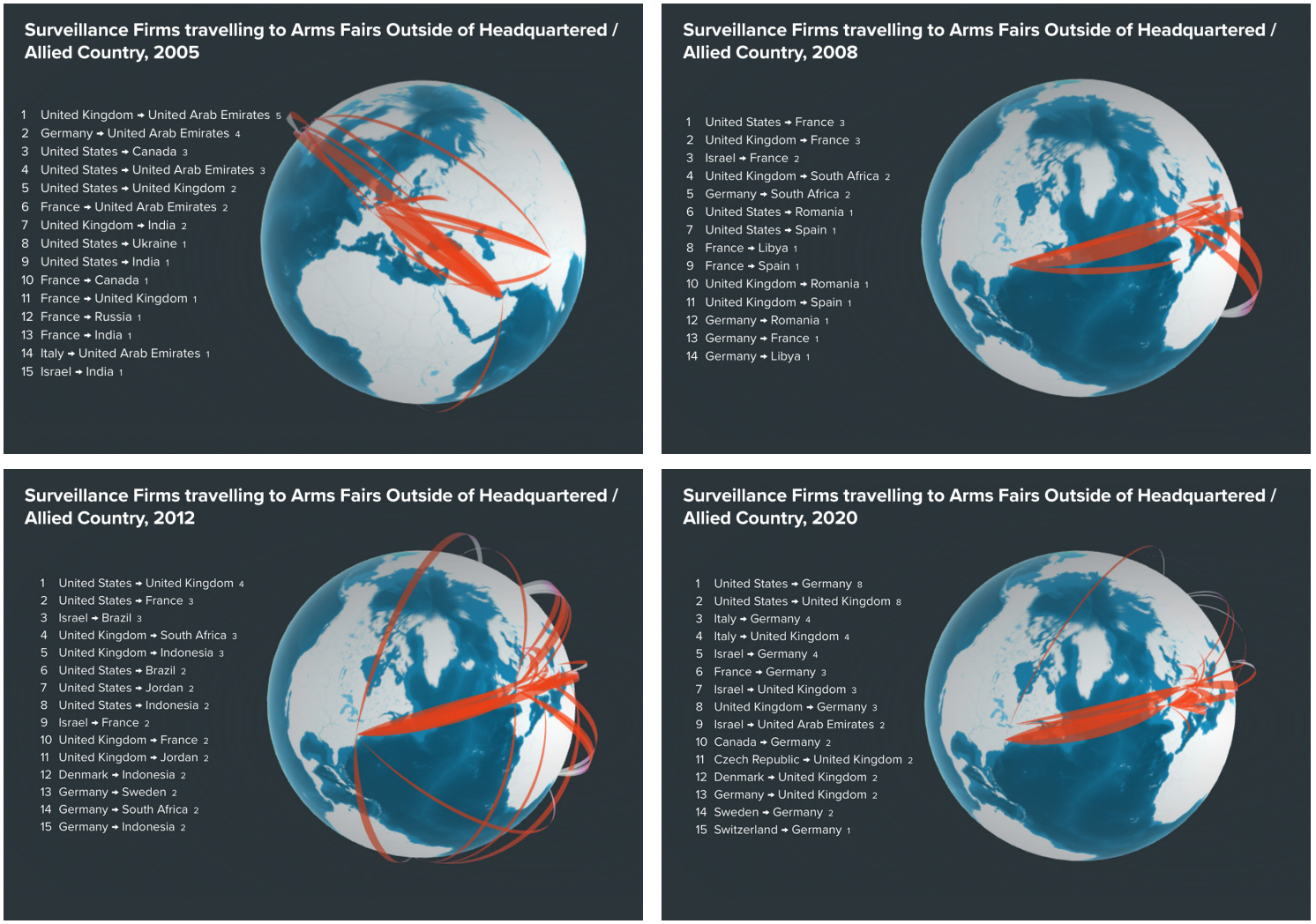
Almost 75 percent of the eighty-one high/medium-confidence companies have exhibited their wares to arms fairs **outside of their home continent** in the last twenty years. More than 85 percent have exhibited at an arms fair outside their home country in the last twenty years. This excludes the two firms headquartered in Five Eyes countries that have only been to arms fairs in a Five Eyes country. (The full list of the sixty firms is in the Appendix.) When broken down by year, this trend remains consistent; of all the firms marketing to arms fairs in a given year, more firms market to arms fairs outside their continent in a given year than restrict sales to their continent or country.

Figure 4.



https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#numbertraveling

Figure 5.



https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#globalattendance

Above is a visualization of the arms fair marketing data over time, showing a clear globalization trend. The unidirectional lines represent firms in one country travelling to an arms fair in another in a single year, and the thickness of the lines represents the number of firms making this trip. This visualization excludes lines between Five Eyes countries. As seen in the visualization, many trips made over the last twenty years by vendors in this space consistently include Europe and the Middle East. The number and variety of trips are also growing, displaying partnerships between countries that have no set intelligence alliances. As companies travel and market to new continents and new countries, the already worrying pace of offensive cyber capability proliferation may quicken.

Any capabilities sold to non-ally countries carry a risk: these capabilities could eventually be used to target individuals and organizations in one's home country. This risk has notably played out in the Project Raven case, in which the US contractor CyberPoint built up cyber capabilities in the United Arab Emirates. Subsequently, the Emirati government used those capabilities to spy on US citizens, among others.[32] CyberPoint and its Emirati descendant DarkMatter (which took over the Project Raven program) are both featured in this dataset. Both organizations marketed to ISSWorld Middle East and arms fairs within the UAE—CyberPoint from 2013–2015, and DarkMatter from 2016–2017.

Company	Confidence	HQ	2013	2014	2015	2016	2017
CyberPoint	High	USA	IDEX UAE	ISSWorld Middle East	ISSWorld Middle East		
DarkMatter	High	UAE				ISSWorld Middle East	ISSWorld Middle East, Dubai Airshow, IDEX UAE

3. Which arms fairs (and arms fair host countries) host the most high/medium-confidence firms?

While the two hundred and twenty-four companies in the dataset hail from thirty-three separate countries, most of the companies congregate at a small number of arms fairs, many of which are located in Europe. Milipol France and Security & Policing Home Office (based in the UK) are the two most widely attended arms fairs for the high/medium-confidence firms selling interception/intrusion capabilities. This is likely due to size and specialization, respectively. Milipol France is one of the world's largest arms fairs, with more than one thousand exhibitors, while Security & Policing has a track dedicated to cybersecurity.[33]

France and the UK are also the top countries where high/medium-confidence firms congregate, mostly due to the two aforementioned conferences. Germany, Singapore, Qatar, and Israel are also common destinations for high/medium-confidence firms, while the United Arab Emirates and the United States play host to more firms overall, thanks to a variety of smaller arms fairs.

	Conference	Country	# High/medium confidence	Total companies
1	Milipol France	France	54	108
2	Security and Policing Home Office	United Kingdom	34	78
3	GPEC	Germany	17	35
4	Milipol Qatar	Qatar	14	42
5	Milipol Asia	Singapore	12	27
6	Security and Counter Terror Expo	United Kingdom	10	24
7	DSEI	United Kingdom	9	40
8	HLS & Cyber	Israel	8	17
9	Shield Africa	Ivory Coast	8	15
10	ISDEF	Israel	7	20

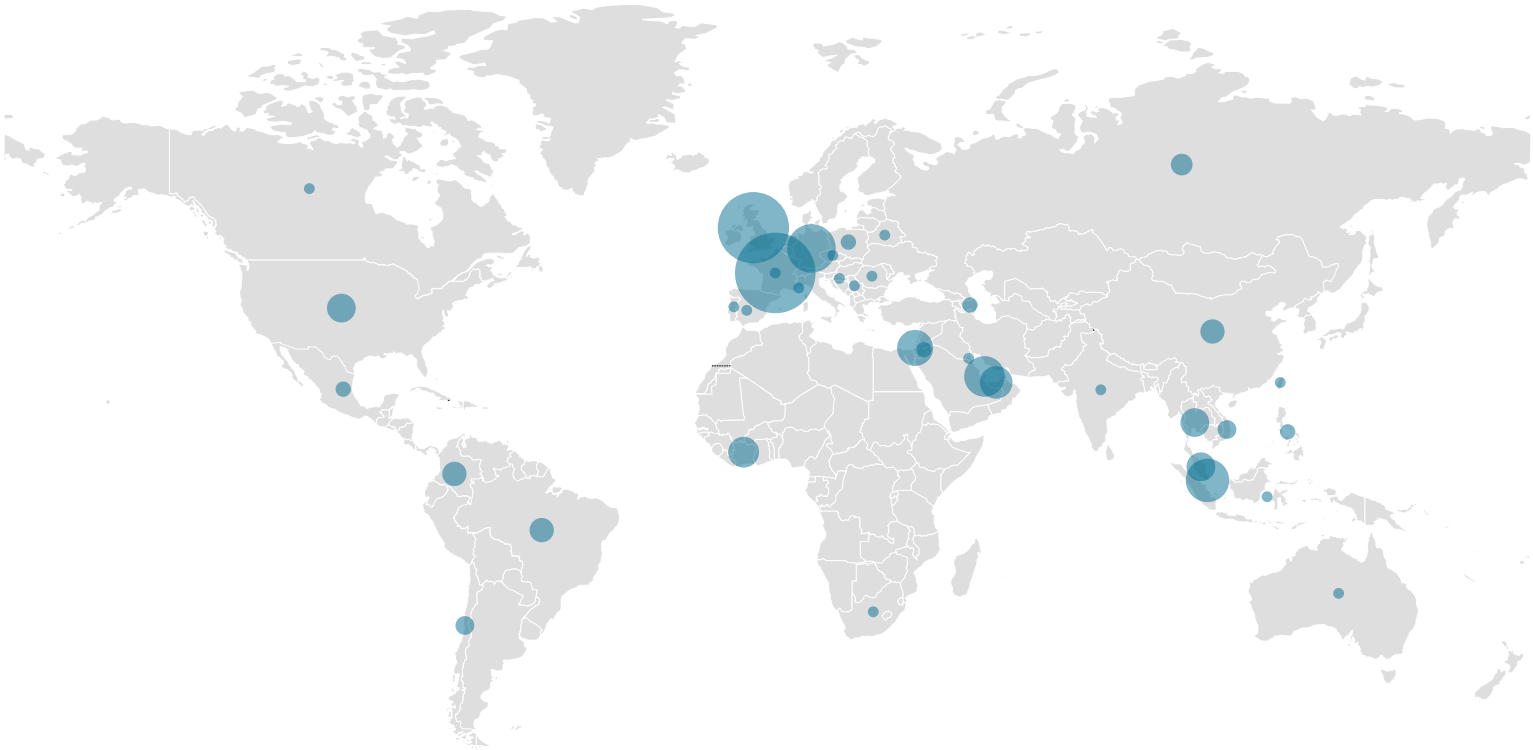
4. What companies are marketing interception/intrusion capabilities to US and NATO adversaries?

Five of the eighty-one high/medium-confidence firms have attended arms fairs in Russia and China as exhibitors in the last twenty years.[34] The authors believe that by selling to these parties, these organizations are willing to accept or ignore the risk that their products may bolster the capabilities of adversary governments, who may use their products to conduct espionage more effectively. For example, Cellebrite, a well-known Israeli firm, has consistently been an exhibitor at arms fairs in both China and Russia from 2013 onward, and is the only firm in the dataset to attend a Chinese arms fair multiple times in the last five years. Cellebrite, which sells software to physically extract and index data from mobile devices, is known to have both Chinese and Russian customers.[35]

Some of the other firms in the below tables have received less media attention than Cellebrite, but are no less concerning. BTT is a Turkish firm that has assisted Turkish law enforcement with call-detail record collection.[36] In a 2017 Al Jazeera investigation of the spyware market, BTT representatives claimed to use a wide interpretation of "telecommunications equipment" in order to circumvent export-control paperwork.[37] MSAB, a firm that has also marketed to both Russia and China, sells mobile forensics products that have been used against activists in Hong Kong and Myanmar.[38]

Figure 6.

Arms Fair Countries by Number of High / Medium Confidence Exhibitors



https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#armsfairmap

Russia Arms-Fair Attendees	Headquarters	Confidence	Years
BTT	Turkey	Medium	2015, 2016, 2017
Cellebrite	Israel	High	2013, 2015, 2016, 2017, 2018
Micro Systemation AB (MSAB)	Sweden	High	2013, 2015, 2016, 2017, 2018

China Arms-Fair Attendees	HQ	Confidence	Years
Cellebrite	Israel	High	2016, 2017, 2018
Micro Systemation AB (MSAB)	Sweden	High	2016
Verint	Israel	Medium	2013
Vastech	South Africa	Medium	2010, 2011

CONCLUSIONS AND RECOMMENDATIONS

This paper profiles an important set of firms that frequent both ISSWorld and international arms fairs, extracted from an extensive list of vendors operating in the interception/intrusion market. The data from that list show that there are **multiple firms headquartered in Europe marketing capabilities to known Five Eyes/NATO adversaries.** Many of these firms congregate at Milipol France, Security & Policing UK, and other arms fairs within Europe and the Middle East.

For researchers interested in uncovering the dealings of the industry, the authors hope their data and findings can spur further research in this field. And while they do not claim that this is a complete list of potentially irresponsible vendors, or that all identified companies are, in fact, selling indiscriminately, it

is a place to start for regulators interested in tightening control over the industry.

Additional research is needed into some of the lesser-known high/medium-confidence companies in this dataset to uncover their actual products and sales. The difference between publicly marketed products and actual capabilities can differ, and marketing material offers limited insights into both the content and direction of actual sales. Case studies and media reporting have already shown how some firms on this list show a history of transactions with authoritarian regimes, and potentially attempt to evade export controls.[39]

The United States and NATO need to better understand the proliferation of interception/intrusion capabilities; shape the behavior of irresponsible proliferator companies; and limit their activities where they conflict with national security priorities, together with international partners. This work builds on prior research and the understand, shape, and limit framework published earlier this year.[40] The following recommendations are meant to address the growing nation-state market for intrusion/interception capabilities and other forms of surveillance products, rather than all cyber capability proliferation.

To **understand** the current state of intrusion/interception capability proliferation, the United States and NATO member states must work with the companies headquartered in their jurisdiction to encourage sufficient know-your-consumer policies. These policies should also **shape** the behavior of firms, giving firms the power to revoke access to a consumer should the risks associated with that consumer change. Enforcing these policies is both technically difficult (the consumer may reverse engineer and recreate the capability after the service has been revoked, for example), and difficult to enforce (especially among private companies whose internal dealings are opaquer than their publicly traded counterparts). However, working with these organizations whenever possible, rather than against them, will allow governments to develop more collaborative solutions for regulation, while continuing to encourage domestic cyber expertise.

The United States and NATO members must also work more closely with arms fairs held in their jurisdiction to ensure they are aware of any exhibitors that are irresponsible proliferators—i.e., those selling to US/NATO adversaries—and **limit** their ability to attend when possible. Arms fair organizers should be encouraged to ban or limit irresponsible proliferators who are either directly marketing their capabilities to known adversaries, or who have known clients in authoritarian regimes and no KYC policies.

Finally, the United States and NATO members must ensure their export controls actually accomplish what they are intended to do, evaluating both their own export laws and the export laws of countries where irresponsible proliferators are headquartered. This review should lead to a collaborative process with offending countries like Israel, Sweden, and Turkey to both tighten controls around known irresponsible vendors and close loopholes enabling those vendors to circumvent these export controls. Naming and shaming both the vendors and the regimes abusing vendor capabilities to conduct human-rights violations are also encouraged.[41]

The proliferation of cyber and surveillance capabilities is a thorny policy question. Preventing the harms caused by this industry is an important policy goal, and should be treated as such. Yet, attempts at regulating the industry through export regulation and global regimes have had limited success so far. On top of this, this analysis indicates that there exists a significant group of private companies willing to act irresponsibly: marketing capabilities that carry the risk of becoming tools of oppression for authoritarian regimes or strategic tools for non-NATO allies. The United States, NATO, and their allies still have policy tools they can use to prevent privately developed offensive cyber capabilities from proliferating irresponsibly. The continued absence of assertive policy response risks a grim outlook: a growing number of private corporations that see few consequences to bolstering the cyber arsenals of major Western adversaries, and only profit.

APPENDIX A:
Visualization of all companies by arms fairs/ISSWorld conferences attended:
https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#appendices

APPENDIX B:
List of high/medium-confidence companies (full list with low confidence can be found here.)

Company	Irresponsible Proliferator	Confidence Level	Description	Headquarters
3m electronic monitoring	x	High	Electronic monitoring	United States
advanced systems	x	High	Part of Intellexa coalition	United Arab Emirates
aglaya	x	High	Spyware	India
aqsacom	x	High	Lawful interception	France
area	x	High	Surveillance tech	Italy
cellebrite	x	High	Digital forensics	Israel
cleartrail	x	High	Communication analytics solutions	India
cyberpoint	x	High	Trained dark matter	United States
elaman	x	High	Data forensics, intelligence fusion systems	Germany
gamma group	x	High	Spyware	Italy
gita technologies	x	High	Tactical interception, intelligence gathering	Israel
hacking team (memento labs)	x	High	Digital forensics	Italy
innova	x	High	Consultancy	Italy
intelligent computer solutions	x	High	Digital forensics	United States
interionet systems	x	High	Mobile intrusion	Israel
jenovice	x	High	Bluetooth and Wi-Fi interception	Israel
logicube	x	High	Digital forensics	United States
lumacron	x	High	Interception, monitoring, and recording solutions for optical networks	United Kingdom
merlinx (equus technologies)	x	High	Tactical interceptions	Israel
mh service gmbh	x	High	Digital forensics	Germany
neosoft ag	x	High	Lawful interception	Switzerland
nexa technologies	x	High	Various surveillance products	France
norsi-trans	x	High	Information analytics	Russia
nso group	x	High	Spyware	Israel

Company	Irresponsible Proliferator	Confidence Level	Description	Headquarters
pat systems	x	High	IMSI catching, mobile-communication interception	United States
polaris wireless	x	High	Mobile location	United States
pro4tech	x	High	Tactical surveillance	Israel
providence	x	High	Surveillance training and technology	United Kingdom
q cyber	x	High	Spyware	Israel
rayzone group	x	High	Various surveillance products, remote access, network monitoring, SS7 interception	Israel
rcs lawful interception solutions	x	High	Lawful interception	Italy
seartech	x	High	Tactical surveillance	South Africa
securcube	x	High	Forensic consultants, Cellebrite-certified engineers	Italy
septier communications	x	High	Various surveillance products, IMSI catchers	Israel
sio	x	High	Lawful interception	Italy
toka cyber builders	x	High	Cybersecurity	Israel
tracespan	x	High	Broadband monitoring and interception solutions	Israel
trovicor	x	High	Lawful interception and intelligence technology	Germany
utimaco	x	High	Data retention, lawful interception	Germany
wintego	x	High	Cyber intelligence	Israel
wispear	x	High	Wi-Fi intelligence and interception	Cyprus
xci	x	High	Forensics	Denmark
msab	x	High	Mobile forensics	Sweden
adf solutions		High	Digital forensic solutions	United States
cepia technologies		High	Various surveillance products	Czech Republic
comsec		High	Mobile SIGINT	United States
crypton-m		High	Passive GSM interception	Ukraine
darkmatter		High	Cybersecurity	United Arab Emirates
decision group		High	Real-time network forensics and lawful interception	Taiwan
finfisher		High	Spyware	Germany

Company	Irresponsible Proliferator	Confidence Level	Description	Headquarters
forsolution		High	Digital forensics, lawful interception	Czech Republic
gr sistemi		High	Data analytics, intrusion	Italy
hidden technology		High	Covert tracking and surveillance products	United Kingdom
kommlabs		High	Lawful interception	India
paraben corporation		High	Digital forensics	United States
pro4sec		High	SMD modifications	Croatia
ss8		High	Lawful intelligence	United States
syborg		High	Wi-Fi interception	Germany
wolfcyber		High	Spyware	Germany
accessdata	x	Medium	Forensics and data analysis	United States
basis technology	x	Medium	AI, but also vendor for autopsy forensics	United States
bivio networks	x	Medium	DPI	United States
btt	x	Medium	COMINT, intelligence support systems	Turkey
cellxion	x	Medium	VPN, cellular intelligence and geolocation	United States
cy4gate	x	Medium	Lawful interception, cyberwarfare, data management	Italy
darkblue telecommunication systems	x	Medium	Tactical location finding	Turkey
deveryware	x	Medium	Geolocation	France
ip access	x	Medium	IMSI catching, mobile-communication interception	United Kingdom
ips	x	Medium	Communication monitoring and analysis, interception capabilities	Italy
knowlesys	x	Medium	OSINT	China
mobilaris	x	Medium	Mobile location, traffic data	Sweden
nuix	x	Medium	Data analytics, digital forensics	Australia
qosmos	x	Medium	DPI	France
vastech	x	Medium	Cyber intelligence, analytics, tracking	South Africa
vehere	x	Medium	Communications interception, speech intelligence and analytics, cryptoanalysis	India

Company	Irresponsible Proliferator	Confidence Level	Description	Headquarters
verint	x	Medium	Defense contractor	Israel
creativity software		Medium	Mobile location	United Kingdom
evistel		Medium	Geolocation	France
intecs gmbh		Medium	Various surveillance, access technologies	Germany
telesoft		Medium	OSINT, big data, network interception	United Kingdom
vanume		Medium	Monitoring, geolocation, big data	Mexico

ABOUT THE AUTHORS

Winnona DeSombre is a first-year MPP/JD dual degree candidate at the Harvard Kennedy School and Georgetown Law, and a non-resident fellow at the Atlantic Council. Her research interests encompass the proliferation of offensive cyber capabilities, particularly by private sector actors, and cyber security in the East Asian region. Prior to Harvard, Winnona was a security engineer at Google's Threat Analysis Group.

Lars Gjesvik is a doctoral research fellow at the Norwegian Institute of International Affairs and affiliated with the University of Oslo. His research interests are markets in cyber security, data flows, and digital infrastructures. Previously, Lars has written on digital sovereignty, disinformation, and critical infrastructure protection.

Johann Ole Willers is a doctoral research fellow at the Norwegian Institute of International Affairs and affiliated with the Department of Organization at the Copenhagen Business School. His research focuses on markets and experts in cybersecurity. Ole has published on issues such as cybersecurity capacity building, expert profiles, and European Union governance.

Endnotes

1 Patrick Howell O'Neill, "ISS World: The Traveling Spyware Roadshow for Dictatorships and Democracies," *CyberScoop*, June 20, 2017, https://www.cyberscoop.com/iss-world-wiretappers-ball-nso-group-ahmed-mansoor/.

2 Whether a company is a strategic concern, primarily enabling oppression domestically, or both, depends on the exact products and capabilities it provides, and publicly available information gives limited insights into the exact products companies are offering. The authors have included those companies they deem a cause for concern in both regards, based on the information about their products that is openly available, but recognize that these assessments are imperfect.

3 This excludes high/medium-confidence firms headquartered in US/NATO adversary countries marketing to their home country, such as Norsi-Trans, a Russian surveillance firm that frequently markets to its home country.

4 See Page 12.

5 "Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than $1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government," US Department of Justice, press release, September 14, 2021, https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million.

6 Winnona DeSombre, et al., *Countering 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/.

7 Julia Voo, et al., "National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.

8 Andrea Peterson, "Why Everyone Is Left Less Secure When the NSA Doesn't Help Fix Security Flaws," *Washington Post,* October 4, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/.

9 "Convention on Cybercrime," Council of Europe, 2001, articles 19–20, https://rm.coe.int/1680081561; "The EU Funds Surveillance Around the World: Here's What Must be Done About It," Privacy International, September 18, 2019, https://privacyinternational.org/long-read/3221/eu-funds-surveillance-around-world-heres-what-must-be-done-about-it.

10 "Executives of Surveillance Companies Amesys and Nexa Technologies Indicted for Complicity in Torture," Amnesty International, June 22, 2021, https://www.amnestyusa.org/press-releases/executives-of-surveillance-companies-amesys-and-nexa-technologies-indicted-for-complicity-in-torture/.

11 Bill Marczak, et al., "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab, Munk School, and University of Toronto, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/; Stephanie Kirchgaessner, et al., "Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon," *Guardian*, July 18, 2021, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus; Dana Priest, Craig Timberg, and Souad Mekhennet, "Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide," *Washington Post,* July 18, 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/.

12 Christopher Bing and Joel Schectman, "Inside the UAE's Secret Hacking Team of American Mercenaries," Reuters, January 30, 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/.

13 For example: Bill Marczak, et al., "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus." Citizen Lab, Munk School, and University of Toronto, July 15, 2021, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/. The Citizen Lab investigation into the operations of "Dark Basin"—a hack-for-hire group linked to the Indian company BellTrox—has provided evidence that similar tools have eclipsed the state-dominated market and are available on far broader scale. John Scott-Railton, et al., "Dark Basin: Uncovering a Massive Hack-for-Hire Operation," Citizen Lab, Munk School, and University of Toronto, June 9, 2020, https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/; Trey Herr, "Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle," Belfer Cyber Security Project White Paper Series, June 27, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005616; Robert Morgus, Max Smeets, and Trey Herr, "Countering the Proliferation of Offensive Cyber Capabilities," Global Commission on the Stability of Cyberspace, 2017, http://maxsmeets.com/wp-content/uploads/2018/09/GCSC-Briefings-from-the-Research-Advisory-Group_NewDelhi-2017-161-187.pdf; Trey Herr, "Governing Proliferation in Cybersecurity," *Global Summitry* 3, 1, 2017, 86–107, https://doi.org/10.1093/global/gux006; Trey Herr, "Malware Counter-Proliferation and the Wassenaar Arrangement," 8th International Conference on Cyber Conflict, Tallinn, 2016, 175–190, https:// ieeexplore.ieee.org/abstract/document/7529434; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND, 2014, https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf; Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," 4th International Conference on Cyber Conflict, 2012, 91–109, https:// ccdcoe.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf; Joseph Nye, "Nuclear Lessons for Cyber Security?" Strategic Studies Quarterly 5, 4, 2011, 18–38, https://dash.harvard.edu/handle/1/8052146; Kenneth Geers, "Cyber Weapons Convention," *Computer Law & Security Review 26,* 5, September 2010, 547–551, https://doi.org/10.1016/j.clsr.2010.07.005.

14 Tim Maurer, *Cyber Mercenaries* (Cambridge: Cambridge University Press, 2018); David Kaye, "UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools," United Nations Office of the High Commissioner for Human Rights, June 25, 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736; Brad Smith, "A Moment of Reckoning: the Need for a Strong and Global Cybersecurity Response," Microsoft, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/; James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community: Senate Select Committee on Intelligence," March 12, 2013, https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf; David Kaye and Marietje Schaake, "Global Spyware Such as Pegasus is a Threat to Democracy. Here's How to Stop It," *Washington Post*, July 19, 2021, https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/.

15 Joseph S. Nye, "The World Needs an Arms-Control Treaty for Cybersecurity," Belfer Center for Science and International Affairs, October 1, 2015, https://www.belfercenter.org/publication/world-needs-arms-control-treaty-cybersecurity.

16 DeSombre, et al., *Countering Cyber Proliferation.*

17 Marczak, et al., "Hide and Seek"; "Exploiting Vulnerabilities in Cellebrite UFED and Physical Analyzer from an App's Perspective," *Signal Messenger,* April 21, 2021, https://signal.org/blog/cellebrite-vulnerabilities/; Marczak, et al., "Hooking Candiru."

18 Mark Bromley, "Export Controls, Human Security and Cyber-surveillance Technology: Examining the Proposed Changes to the EU Dual-use Regulation," Stockholm International Peace Research Institute, 2017, https://www.sipri.org/sites/default/files/2018-01/sipri1712_bromley.pdf; Morgus, et al., "Countering the Proliferation of Offensive Cyber Capabilities."

19 The authors are greatly appreciative of the Omega Foundation's assistance with this project. Their dataset on arms-fair exhibitors is located at: "Arms Fairs," Omega Research Foundation, https://omegaresearchfoundation.org/resources/arms-fairs.

20 O'Neill, "ISS World."

21 "Arms Fairs."

22 The program checks for an occurrence of the name in both datasets, with either an exact or partial match. The program contained three conditions: if the arms-fair company is an exact match to the ISSWorld company, it was added to the dataset (e.g., "WolfCyber Intelligence" = "WolfCyber Intelligence"); if the arms-fair company started with the name of the ISSWorld company or vice versa, it was added to the dataset (e.g., "WolfCyber" = "WolfCyber Intelligence"); and if the arms-fair company started with the name of the ISSWorld company in parentheses, it was added to the dataset (e.g., "Hacking Team (Memento Labs)" = "Memento Labs"). This was followed by manual cleaning to remove vaguely named companies or other false positives.

23 Dataset is in a Google Sheet: https://docs.google.com/spreadsheets/d/1v3YvimIuj_UtJ8YcCpKDtDuKlu5QN04ajcB9C7dRqH4/edit?usp=sharing.

24 The full log of unfiltered matches can be found in the "debuglog_with_all_matches" tab within the datasheet. While the authors have tried to consolidate acquisitions of corporations, some company rebrandings (e.g., NSO/Q Cyber) remain separate.

25 "Assessing China's Digital Silk Road Initiative," Council on Foreign Relations, December 18, 2020, https://www.cfr.org/china-digital-silk-road.

26 "How to Find the Legal English Name of a Chinese Company," SinoInspection.com, December 24, 2020, https://sinoinspection.com/find-legal-english-name-chinese-company/.

27 Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017; Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," Reuters, March 22, 2012, https://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322.

28 "About Pro4Sec," PRO4SEC Ltd., February 16, 2021, https://pro4sec.com/about/; "Communication Data Analytics—ClearTrail," ClearTrail Technologies, August 17, 2021, https://clear-trail.com/.

29 Lorenzo Franceschi-Bicchierai, "Italian Cops Raid Surveillance Tech Company Accused of Selling Spy Gear to Syria," VICE, December 1, 2016, https://www.vice.com/en/article/gv5knx/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria; Lorenzo Franceschi-Bicchierai, "Government Spyware Vendor Left Customer, Victim Data Online for Everyone to See," VICE, October 24, 2018, https://www.vice.com/en/article/vbka8b/wolf-intelligence-leak-customer-victim-data-online.

30 "Deveryware—Technologies Leader in Investigation and Services for Global Security," Deveryware, July 11, 2021, https://deveryware.com/?lang=en.

31 "Our Story," JENOVICE Cyber Labs, accessed September 21, 2021, https://www.jenovice.com/.

32 Bing and Schectman, "Inside the UAE's Secret Hacking Team of American Mercenaries."

33 "Milipol Paris 2021: Leading Event for Homeland Security & Safety," Milipol France, https://en.milipol.com/; "2021 Exhibitors Archive," Security and Policing UK, https://www.securityandpolicing.co.uk/exhibitors/exhibitors-list-2021/.

34 This excludes any firms also headquartered in Russia and China. For example, Norsi Trans is a high-confidence Russian company that has attended Russian arms fairs in 2009, 2010, 2015, 2016, 2017, 2018, and 2019.

35 "Exploiting Vulnerabilities in Cellebrite UFED and Physical Analyzer from an App's Perspective."

36 "BTT Provides State of the Art Solutions for Turkish Government," *Defence Turkey Magazine,* 2009, https://www.defenceturkey.com/en/content/btt-provides-state-of-the-art-solutions-340.

37 "How the 'Dual-Use' Ruse Is Employed to Sell Spyware," Al Jazeera, April 10, 2017, https://www.aljazeera.com/features/2017/4/10/how-the-dual-use-ruse-is-employed-to-sell-spyware.

38 Hannah Beech, "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown," *New York Times*, March 1, 2021, https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html.

39 Ibid.; "How the 'Dual-Use' Ruse Is Employed to Sell Spyware."

40 DeSombre, et al., Countering Cyber Proliferation.

41 Ibid.

Atlantic Council

Board of Directors