



**Countering Cyber Proliferation:
Zeroing in on Access-as-a-Service**

WINNONA DESOMBRE,
MICHELE CAMPOBASSO,
LUCA ALLODI, JAMES SHIRES,
JD WORK, ROBERT MORGUS,
PATRICK O'NEILL, AND TREY HERR

Scowcroft Center for Strategy and Security

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Cyber Statecraft Initiative

The **Cyber Statecraft Initiative** 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

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations.

The Atlantic Council, its partners, and funders do not determine, nor do they necessarily endorse or advocate for, any of this report's particular conclusions.

© 2021 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

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



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Countering Cyber Proliferation: Zeroing in on Access-as-a-Service

WINNONA DESOMBRE, MICHELE CAMPOBASSO,
LUCA ALLODI, JAMES SHIRES,
JD WORK, ROBERT MORGUS,
PATRICK O'NEILL, AND TREY HERR

ISBN-13: 978-1-61977-161-1

Cover: The Pandora's Box of Cyber Proliferation. Source: Sarah Orio

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

March 2021

Table of Contents

- Executive Summary** 1
- Introduction** 2
- Offensive Cyber Capability Proliferation: a Quick Review** 6
 - The Five Pillars of Offensive Cyber Capability Proliferation..... 7
- Case Studies** 8
 - 1. NSO Group..... 8
 - 2. ENFER11
 - 3. DarkMatter Group.....14
- Previous Approaches to Countering Proliferation of OCC**.....17
- Countering Proliferation Policy Recommendations**19
 - 1. UNDERSTAND & PARTNER.....19
 - Recommendation 1.1: Build a coalition of like-minded partners..... 20
 - Recommendation 1.2: Elevate the issue of offensive cybersecurity capabilities proliferation in international forums..... 20
 - Recommendation 1.3: Pass “Know Your Vendor” laws or regulations 20
 - 2. SHAPE21
 - Recommendation 2.1: Develop ban lists for vendors that are caught selling capabilities to states or entities on published lists of concern.....21
 - Recommendation 2.2: Standardize risk assessment for the AaaS industry.....21
 - Recommendation 2.3: Incentivize corporate ethics committees22
 - Recommendation 2.4: Limit foreign military sales and other foreign assistance to states that purchase from banned AaaS providers or use AaaS tools to infringe on human rights.....22
 - 3. LIMIT23
 - Recommendation 3.1: Widen the scope of selective defensive vulnerability disclosure23
 - Recommendation 3.2: Establish post-employment restrictions for former government cybersecurity employees23
 - Recommendation 3.3: Pursue legal action against AaaS providers and subcontractors24
 - Recommendation 3.4: Encourage technical limits on malware payload jurisdiction.....24
- Conclusion**.....25
- About the Authors**26

For more on Offensive Cyber Capabilities and the private marketplaces where they proliferate, check out our associated Primer: *A Primer on the Proliferation of Offensive Cyber Capabilities*

Executive Summary

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. As these capabilities become more prolific, their regulation through formal international norms and export controls is increasingly ineffective. Countering the spread of dangerous capabilities is not a new policy challenge, but its specific application to the cyber domain remains uncertain both in theory and in practice. Left unchecked, the continued proliferation of OCC could significantly damage the global economy, international security, and the values that the United States and its allies hold dear. Thus, it is imperative that governments reevaluate their approach to countering the proliferation of OCC. This report profiles the “Access-as-a-Service” (AaaS) industry, a significant vector for the proliferation of OCC, as a means of both illustrating the character of this proliferation and investigating policies to counter it.

AaaS firms offer various forms of “access” to target data or systems, and through these business practices are creating and selling OCC at an alarming rate. These companies advertise their wares to myriad groups, mostly states, who would not otherwise be able to develop such capabilities themselves. AaaS products and services vary in form, but share foundations that can be categorized under five “pillars” of OCC: *Vulnerability Research and Exploitation*, *Malware Payload Development*, *Technical Command and Control*, *Operational Management*, and *Training and Support*.

Framed along these pillars, the authors present three case studies (the NSO Group, ENFER, and DarkMatter) to illustrate the complexity of the overlapping activities within the self- and semi-regulated markets of the AaaS industry. These companies operate within a semi-regulated market, functioning openly and legally under the jurisdiction of their country of operation. Together, their activities cover the full spectrum of OCC development described in five pillars below. They are also significant cases for policy-maker attention spanning back almost a decade. **NSO Group** is an Israeli firm that offers services, including targeted surveillance software, to multiple government clients. NSO software has been connected to multiple human rights abuses, particularly against journalists

covering and operating in the Middle East, and is, at the time of this report, the subject of a lawsuit by several leading US technology companies. **ENFER** (a cryptonym), is a contractor operating in the Russian Marketplace, which allegedly partakes in offensive operations under the direct instruction of the Russian Federal Security Service (FSB). **DarkMatter** is located in and operates under the jurisdiction of the United Arab Emirates (UAE), but originated in a collaboration with US contractors through Project Raven (under which former US intelligence operatives were recruited by the UAE for surveillance activities). DarkMatter appears to take a larger role, comparatively, in operational targeting and is tightly associated with key UAE intelligence agencies.

The report uses these three cases to derive several policy recommendations for states to better **understand** this proliferation of OCC, **shape** the behavior of these companies, and **limit** their activities where it conflicts with national security priorities, together with international partners. To better understand this proliferation, states should create “know your vendor” laws requiring AaaS firms to identify all their vendors and customers before selling their services to governments. To more effectively shape behavior, the report recommends states widen the scope of selective disclosure to include the capabilities developed and sold by selected AaaS firms and ban vendors that fail to adhere to “know your vendor laws.” States should also implement contracting preferences for those which adhere to these laws, and develop standards on which firms can map self-regulatory schemes, including ethics committees. Finally, where states see an overriding national security need to limit the proliferation of OCC through these firms, they can introduce more rigorous post-employment reporting for certain intelligence and cybersecurity-specific roles in the public sector. Additionally, they can work with firms to impose technical limitations on OCC, like geofencing and registered customer lists.

Implementing these recommendations would create crucial tools for states to better counter the proliferation of OCC through the activities of AaaS firms. These are initial steps; the larger counterproliferation effort will be a longer process as these products and their customer base evolve. And while this is not the first time concerns have been raised around such problematic activities, earlier policy attention had largely been focused on the human rights implications of offensive cyber capabilities, leveraged by authoritarian states or

through abuse of weak operational controls in the absence of effective oversight. The interactions within this emerging market have contributed to compromises of critical national infrastructure and driven the development of new offensive programs by states that had otherwise been unable to rely upon the transfer of key tooling, expertise, and instruction by allied and partner military intelligence services.

These issues however involve a greater range of national security equities; this accordingly demands an expanded conversation and that we elevate the priority in addressing

challenges of Access-as-a-Service associated OCC proliferation. International cooperation will be crucial, as no country is a large enough customer or jurisdictional home for AaaS firms to make a systematic difference alone. The United States and the European Union (EU) in particular have an opportunity to work in concert to understand, shape, and limit this proliferation over the next decade, as public-private links with the research community strengthen and the harms of OCC proliferation continue to sharpen in the public consciousness.

Introduction

The proliferation of offensive cyber capabilities occurs largely uncontrolled. Unlike their nuclear counterparts, cyber capabilities are easier for states to access and use. State cyber capabilities, and the people that build them, can also become a form of proliferation. Offensive capabilities like EternalBlue, allegedly engineered by the United States, have already been reused by the Russian, North Korean, and Chinese governments.¹ Moreover, former US government cyber security professionals are regularly recruited by foreign firms. US sweat equity has contributed to cyber capabilities used to target US citizens on more than one occasion.² Recognizing the problem, but struggling to manage it, the CIA issued a notice which received widespread attention in January 2020, warning former intelligence officers against working for foreign governments.³ The national security implications of unlimited proliferation are well recognized, but states are confronted by the need to do more than simply limit what moves from government to the private sector or between states.

The ability to develop an effective and targeted cyberattack is not only in the hands of states. States entering the cyber domain now find that they can purchase cyber capabilities at scale from private companies within a growing hacker-

for-hire or AaaS industry. These companies, sometimes also labelled “Intrusion-as-a-Service”⁴ organizations, often offer access—to target data, a target account, or sets of mobile devices—as a service. They help drive the spread of cyber capabilities, resulting in increased adversary cyberattacks. These firms represent channels through which ever more potent offensive cyber capabilities can proliferate. By virtue of this proliferation, states extend their operational reach, enhance their efficacy against widely used technologies, and provide greater leverage to their strategic aims. The result is that present tensions and efforts contradictory to the interests of the United States and allies in the EU are magnified while new threats emerge.⁵

For the United States, home to many of the technology providers compromised by these OCC and source of the talent and human skills subject to some of the most widely profiled examples of this proliferation, the problem posed here is neither theoretical nor disconnected from other national security activities. US provision of assistance to allied governments and third parties in the form of offensive technologies has long been tricky, witness the decades-long attempt to recover Man Portable Air Defense Systems

1 Gil Baram, “The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat,” Council on Foreign Relations, 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, April 25, 2017, <https://www.recordedfuture.com/shadow-brokers-malware-release/>; and Leo Varela, “EternalBlue: Metasploit Module for MS17-010,” Rapid7, May 19, 2017, <https://blog.rapid7.com/2017/05/20/metasploit-the-power-of-the-community-and-eternalblue/>.

2 Christopher Bing and Joel Schectman, “Inside the UAE’s Secret Hacking Team of American Mercenaries,” Reuters, January 20, 2019, <https://www.reuters.com/investigates/special-report/usa-spying-raven/>.

3 Julian E. Barnes and Maggie Haberman, “CIA Warns Former Officers about Working for Foreign Governments,” *New York Times*, January 26, 2021, <https://www.nytimes.com/2021/01/26/us/politics/intelligence-officers-foreign-governments.html>.

4 “CyberPeace Institute Calls for Accountability of Intrusion as a Service Sector,” the CyberPeace Institute, December 24, 2020, <https://medium.com/the-cyber-peace-institute/cyberpeace-institute-calls-for-accountability-of-intrusion-as-a-service-sector-clc5597864c3>.

5 The EU is the focus of this discussion as what little existing regulatory apparatus applies to OCC can be found in export controls and other restrictions on commercial activity. NATO, while an important alliance structure and forum for international security, is less directly concerned with these activities and so not the focus of this analysis.

(MANPADS) or more recent effort to stymie the flow of small arms and mine-resistant vehicles across the Middle East.⁶ OCC present this risk of resale and reuse but may also build the capacity of their ultimate recipients in knowledge, training, and skills. This human capital and understanding enables adaptation or further development of these capabilities beyond that initially transferred. Without greater understanding and caution to shape this proliferation, the US risks seeding unintended offensive cyber programs beyond its sphere of influence with little effort.

From a European perspective, as both a producer and influential regulator of offensive cyber capabilities, the sale of OCC acts as a useful lubricant for EU member states' global defense and diplomatic relationships and an easy extension to a strong market in other law enforcement and security sector technologies. But OCC sales, especially to regimes with poor human rights records, are also an increasingly polarized point of contention between both EU member states with varying stakes in the market, and different blocs in the European Parliament.

Current European efforts to carve out a third way between Chinese and US technospheres have so far depended on the strength of its privacy regulation and broader human rights protections, but are beginning to be framed in terms of EU "strategic autonomy," highlighting a clear national security rationale for the control of OCC proliferation. Closer to home, EU cooperation with its southern neighbors across the Mediterranean—often conducted in terms of "security sector reform"—combines both human rights and national security justifications for careful transfer of cyber capabilities, especially as southern EU states such as Spain, Italy, and Greece are drawn closer into geopolitical divisions in the Middle East. NATO offers scant assistance here, as its member states include Turkey, whose approach

to OCC positions it as more of a proliferation concern than a regulatory ally. And Brexit complicates the picture still further, as the United Kingdom (UK) could seek to align with US policy or exploit its new freedom to undercut emerging EU standards.

The profusion of commercial OCC vendors, left unregulated and ill-observed, poses national security risks. For states that have strong OCC programs, proliferation 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—for instance while conducting cyber-espionage for commercial or intelligence gain, or more disruptive or damaging operations.⁷ For states that do not already possess OCC, others' use of OCC is a source of risk and their acquisition is often an attempt to address this imbalance.

OCC proliferation can also threaten human rights, both individual and collective. OCC have been used for intelligence collection by organizations that have subsequently engaged in the arbitrary detention, mistreatment, and torture of those targeted, as well as part of broader campaigns of surveillance and suppression of dissent. This 'human rights' risk does not always align with the national security risk outlined previously—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 posed by the proliferation of offensive cybersecurity capabilities. These risks include both what Lin and Trachtman term "vertical" uses (by states against their own populations) and "diagonal" uses (against the populations of other states, including diaspora).⁸

6 Molly Moore, "CIA Falters in Recovery of Missiles," *Washington Post*, March 7, 1994, <https://www.washingtonpost.com/archive/politics/1994/03/07/cia-falters-in-recovery-of-missiles/73a9a4d7-2952-4077-9746-46bd2e5b81ca/>; Ken Silverstein and Judy Paternak, "A Market for Missiles for Terror," *Los Angeles Times*, March 6, 2003, <https://www.latimes.com/archives/la-xpm-2003-mar-06-fg-sams6-story.html>; Matt Schroeder, "Global Efforts to Control MANPADS," SIPRI Yearbook, Stockholm International Peace Research Institute, 2007, <https://www.sipri.org/sites/default/files/YB07%20623%2014A.pdf>, p. 636; Nima Elbagir, Salma Abdelaziz, Mohamed Abo El Gheit, and Laura Smith-Spark, "Sold to an Ally, Lost to an Enemy," CNN, February 2019, <https://www.cnn.com/interactive/2019/02/middleeast/yemen-lost-us-arms/>; and C.J. Chivers, "How Many Guns Did the U.S. Lose Track of in Iraq and Afghanistan? Hundreds of Thousands," *New York Times Magazine*, August 24, 2016, <https://www.nytimes.com/2016/08/23/magazine/how-many-guns-did-the-us-lose-track-of-in-iraq-and-afghanistan-hundreds-of-thousands.html>.

7 We do not distinguish between espionage, disruption, and destruction here, as it is difficult to disentangle preparation for each in practice, and requires close assessment of specific targeting and malware potential, as well as broader strategic objectives. See, for instance: Ben Buchanan, Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis," *Texas National Security Review*, Fall 2020, <https://tnsr.org/2020/10/preparing-the-cyber-battlefield-assessing-a-novel-escalation-risk-in-a-sino-american-crisis/>.

8 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>

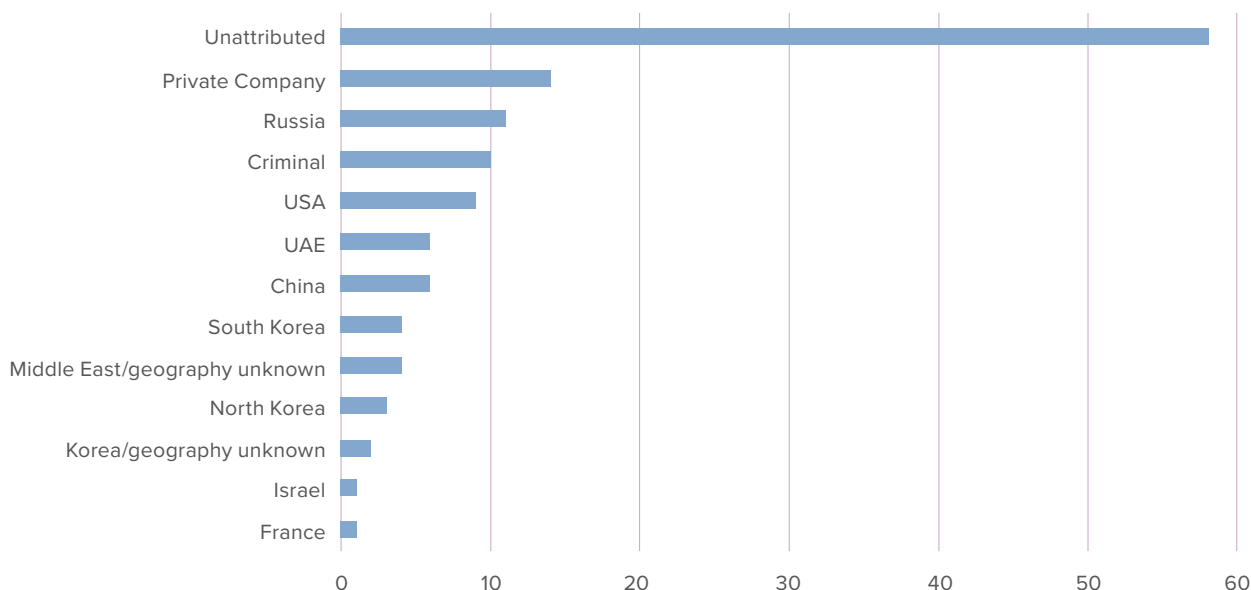
One place in which we see this disturbing trend is in the exploitation of zero day vulnerabilities. A zero day vulnerability is a flaw within a system for which there is no fix at the time of discovery. In 2020, Google's Project Zero published a list of zero day (Oday) exploits discovered in the wild⁹ from 2014 onwards. While only seventy-two of those 129 Odays have been publicly attributed to any threat group, fourteen of these seventy-two, collectively more than any single state, are attributed to private companies: Lench IT Solutions (the creators of commercial surveillance malware FinFisher), Exodus Intelligence, NSO Group, and Hacking Team.

Many of the same companies mentioned above provide training at conferences (or exclusive training upon request), and have developed tailored capabilities for their customers, some of which include Odays.¹⁰ Other similar groups set up their own technical command-and-control infrastructure,

or assist government organizations with operational management processes.

All of these activities fall under the broad term of OCC: a combination of technological, individual, organizational, and infrastructural elements that jointly enable operations in the cyber domain. Companies offer AaaS by combining most, if not all, elements into a single service for clients. Currently, AaaS companies proliferate the full range of offensive cyber capabilities by effectively selling fully fledged services and capabilities alongside detailed training, resulting in a scale of proliferation not seen in government or criminal spaces.¹¹ As this model becomes increasingly common among private firms, the shortfalls of previous policy interventions focusing on the sale or transfer of specific technologies become more glaring, highlighting the need for a more granular and systematic treatment of both these transactions and the

GRAPH 1: Number of Odays publicly found exploited in the wild by attributed threat group category / geography.



Data taken from Google's Project Zero database.¹ More information on Project Zero's visibility into Odays in the wild can be found on the Project Zero website.²

1 "Oday 'In the Wild,'" Google Project Zero, last updated January 14, 2021, <https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRxdtuPLCII7mIUreokfSgajnSyY/edit?usp=sharing>.

2 Ben Hawkes, "Oday 'In the Wild,'" Project Zero, May 15, 2019, <https://googleprojectzero.blogspot.com/p/Oday.html>.

9 "Oday 'In the Wild,'" Google Project Zero, last updated January 14, 2021, <https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRxdtuPLCII7mIUreokfSgajnSyY/edit?usp=sharing>.

10 "On the WhatsApp Oday and Legal Action Against NSO Group," Nex, May 14, 2019, <https://nex.sx/blog/2019/05/14/on-whatsapp-oday-legal-action-nso.html>.

11 In this way, AaaS companies can act as proxies for state proliferation, which is the main focus of international relations literature on OCC proliferation. See, for example: Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge New York: Cambridge University Press, 2018); and Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, Massachusetts: Harvard University Press, 2020).

industry as a whole. This scrutiny appears welcome by some major players in the technology industry, with Microsoft joining others in an amicus brief in support of a case brought by Facebook against NSO Group for capabilities the firm developed and sold targeting the WhatsApp communications service.¹²

Analyzing AaaS helps us investigate more broadly a larger set of policy levers across OCC, as well as more accurately represent the environment these companies and their customers operate in. This proliferation of cyber capabilities is an urgent issue for the United States and allies, including the European Union and its member states. The current status quo of patchwork regulation and fragmented international policy initiatives does not meaningfully address any of the threats posed to human rights or national security interests by this proliferation. This paper provides a concise summary of the content of the AaaS market, profiles three prominent vendors (Israel's NSO Group, a contractor for the Russian Ministry of Defense that we label ENFER for this discussion, and the UAE firm DarkMatter), and offers a policy framework for states to more effectively understand, shape, and limit the

activities of this market within the limits of their jurisdiction and laws.¹³ These three cases are far from the only vendors in the AaaS marketplaces, nor are they the only ones actively developing these capabilities. Rather, they serve as representative cases of certain types of firms and together engage in transactions covering all the pillars of offensive cyber capability development.

The next section provides an overview of the five pillars for OCC that is key to understanding the subsequent case studies section, which breaks down the AaaS actors across the proposed five pillars. Each of these cases, all private sector AaaS firms, showcase a different threat from cyber proliferation: an Israeli firm exploiting US technology companies to help foreign governments violate human rights, a Russian firm making FSB offensive operations stealthier and more dangerous, and an Emirati firm actively recruiting former members of the US intelligence community to spy on neighbors and allies. The paper then analyzes previous approaches to countering OCC proliferation and provides forward-looking policy recommendations tackling the core aspects highlighted within the five pillars of OCC.

12 Catalin Cimpanu, "Microsoft, Google, Cisco, and Others File Amicus Brief in Support of Facebook's NSO Lawsuit," December 21, 2020, <https://www.zdnet.com/article/microsoft-google-cisco-and-others-file-amicus-brief-in-support-of-facebooks-nso-lawsuit/>; "NSO Group Technologies LTD. et al. v. WhatsApp Inc. et al.," No. 20-16408 (9th Cir. Northern District of California), December 21, 2020, <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf>.

13 Both NSO Group and ENFER engage in at least four of the five AaaS aspects, with only operational management and control potentially outside their scope. DarkMatter likely engages in four, if not all five.

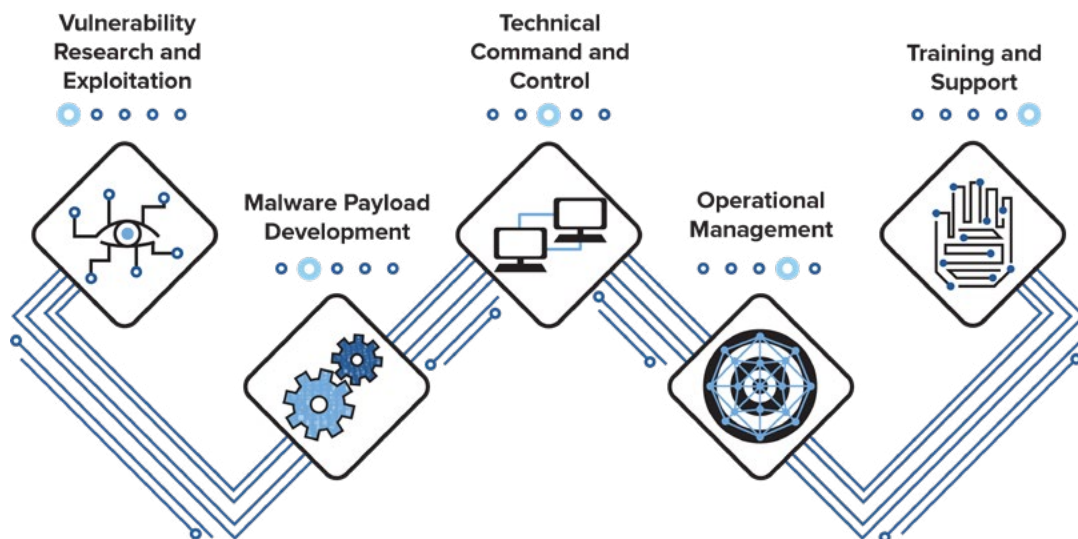
Offensive Cyber Capability Proliferation: a Quick Review

Containing, controlling, or slowing the spread of cyber capabilities is not a new policy challenge. Similar actions have long been undertaken to contain the spread of nuclear, chemical, and biological weapons, commonly referred to as counter- and non-proliferation efforts. These regimes and their applicability to the proliferation of offensive cyber capabilities have been addressed going back a decade in academic and policy literature with minimal tangible progress.¹⁴ Countering the proliferation of offensive cyber capabilities encompasses a variety of actor activity and behaviors spanning both illicit and commercial markets. The former usually take place in the criminal underground and operate in largely self-regulated spaces (a dynamic similar to that of certain criminal communities tightly controlling access to small arms¹⁵), whereas

the latter take place out in the open and are largely regulated by local or national laws, as their operation may be affected by the broader geopolitical setting (e.g., for technology export). Naturally, due to their different regulatory nature, different policies are needed to address these two spaces.

Nonetheless, OCC at large are built on top of a common foundation emerging from five technological and operational pillars that, together, characterize the nature of the developed offensive capabilities. These five pillars of cyber capability proliferation can be used to characterize capabilities in government, criminal, and private industry sectors, as well as in AaaS firms, regardless of whether these different actors operate in either self- or semi-regulated spaces, or in both.

THE FIVE PILLARS OF OFFENSIVE CYBER CAPABILITY PROLIFERATION



¹⁴ Trey Herr, "Development and Proliferation of Offensive Weapons in Cyber-Security," in *Cyber Weaponry*, ed. Henry Prunckun, (Springer, Cham, 2018), 125–141; 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," GCSC Issue Brief, Memo, 2017, http://maxsmeets.com/wp-content/uploads/2018/09/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017-161-187.pdf; Trey Herr, "Governing Proliferation in Cybersecurity," *Global Summitry* 3, no. 1 (2017): 86-107, <https://doi.org/10.1093/global/gux006>; Trey Herr and Ryan Ellis, "Disrupting Malware Markets," in *Cyber Insecurity: Navigating the Perils of the Next Information Age*, eds. Richard M. Harrison and Trey Herr, (Rowman & Littlefield Publishers, October 18, 2016), https://www.google.com/books/edition/Cyber_Insecurity/NAp7DQAAQBAJ?hl=en&gbpv=0; 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 Corporation, 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://ccdc.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf; Joseph Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 18-38, <https://dash.harvard.edu/handle/1/8052146>; and Kenneth Geers, "Cyber Weapons Convention," *Computer Law & Security Review* 26, no.5 (September 2010): 547-551, <https://doi.org/10.1016/j.clsr.2010.07.005>.

¹⁵ P.J. Cook, J. Ludwig, S. Venkatesh, & A.A. Braga, "Underground gun markets," *The Economic Journal*, 117(524), F588-F618, 2007.

THE FIVE PILLARS OF OFFENSIVE CYBER CAPABILITY PROLIFERATION

Cyber capabilities exist in many forms, including knowledge, personnel, and skills—less tangible than a nuclear fuel rod or even a Kalashnikov. This report’s companion primer details the development of these different forms of OCC across actors operating in both self-regulated and semi-regulated spaces. The primer provides an extensive breakdown of the identified five pillars and their relation to different actors in the threat landscape. The following is an overview.

- 1 Vulnerability research and exploitation:** *Individuals, and sometimes small teams, find vulnerabilities (security holes in software and hardware systems) and write exploits (code that takes advantage of a vulnerability and can lead to the violation of the security policies enforced on a system) to gain additional footholds or access on a target program or device. This is usually done within the context of a multi-stage operation. This pillar includes the vulnerabilities themselves, as well as the disclosure programs and research organizations that facilitate the proliferation of discovered vulnerabilities and written exploits.*
- 2 Malware payload development:** *The central part of many offensive cyber campaigns is malware (i.e., the malicious payload executed on the vulnerable system after exploitation, also known as a “virus” or “implant”). This pillar includes any malware and malware tools written or used by attackers to conduct offensive cyber operations, or any endeavor that encourages or conducts exchange of malware.*
- 3 Technical command and control:** *This pillar includes the provision of technologies aimed at supporting the operative aspects of OCC, such as bulletproof hosting, domain name registration, server side command-and-control software, VPN services, and delivery accounts involved with the initial creation of an offensive cyber operation.*

- 4 Operational management:** *The more human-centric aspect of operations, this pillar includes operations management, strategic organization of resources and teams, initial targeting decisions, and other functions that are required to effectively manage an organization that conducts cyber operations.*
- 5 Training and support:** *Offensive cyber operations programs require trained professionals for the programs to be successful. This pillar encompasses any training program or education provided by one set of individuals to another about the offensive cyber operation process, expanding the number of trained professionals and creating connections that facilitate the growth of OCC.*

Each of the pillars contain software, tools, and organizational programs that enable sharing capabilities across borders, by trade or free flow of information. This five pillar model is broader than the technologies considered by the Wassenaar Arrangement, an international export agreement for dual-use technologies modified in 2013 in an attempt to counter the proliferation of what it termed “intrusion software.” Currently, Wassenaar only controls items in Pillar 3 (technical command and control),¹⁶ although a previous iteration did constrain elements of Pillar 1 (vulnerability research and development) and Pillar 2 (malware payload development) before persistent opposition from researchers and industry forced changes.¹⁷ Pillars 4 and 5 were not addressed by either version of Wassenaar, as the arrangement focuses on dual-use technologies rather than wider individual skills and organizational capabilities.

In this study, we focus on three AaaS firms largely operating in semi-regulated, not self-regulated, spaces. We do so because AaaS firms in semi-regulated spaces are the source of many significant offensive cyber capabilities, although they are not the only ones.¹⁸ Firms in semi-regulated spaces are also an easier target of policy intervention. AaaS firms in semi-regulated spaces encompass all forms of OCC proliferation and are becoming increasingly common.

16 For more detail on these discussion, see: Tim Maurer, Edin Omanovic, and Ben Wagner, *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*, New America Foundation, Open Technology Institute, Digitale Gesellschaft, and Privacy International, March 2014, <https://www.newamerica.org/oti/policy-papers/uncontrolled-global-surveillance-updating-export-controls-to-the-digital-age/>; and Collin Anderson, *Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies*, Access, 2015, <https://www.accessnow.org/cms/assets/uploads/archive/Access%20Wassenaar%20Surveillance%20Export%20Controls%202015.pdf>.

17 For Pillar 1, industry practitioners were concerned that the Wassenaar Arrangement would inhibit legitimate vulnerability research, and, for Pillar 2, that it would prevent the transfer of “penetration testing” tools across national borders. For push back, see: Sergey Bratus, D.J. Capelis, Michael Locasto, and Anna Shubina, “Why Wassenaar Arrangement’s Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk – And How to Fix It,” Dartmouth University, October 9, 2014, <https://www.cs.dartmouth.edu/~sergey/wassenaar/wassenaar-public-comment.pdf>.

18 Both NSO Group and ENFER engage in at least four of the five AaaS aspects, with only operational management potentially outside their scope. DarkMatter likely engages in four, if not all five.

Case Studies

The three case studies considered in this paper—Israel’s NSO Group, Russian Ministry of Defense (MoD) contractor ENFER, and the United Arab Emirates firm DarkMatter—are each representative, in different ways, of the broader landscape of AaaS. NSO Group is widely considered a leader in the field, marketing “advanced” AaaS technologies to customers worldwide, and has a significant public profile due to the association of its technologies with human rights violations. ENFER operates in Russia, another important geographical site for AaaS with high policy relevance for the United States, and represents the overlap between semi-regulated and self-regulated, or criminal, markets for AaaS. The DarkMatter case study captures a common transition from dependence on US expertise and technologies to independent AaaS development under the direction of a single state customer and outside the scope of current international regulatory efforts. The basic characteristics of the three cases studies can be seen in Table 1.

1. NSO GROUP

Introduction and background

NSO Group, arguably the most famous of the three case studies, is an Israeli firm alleged to be exploiting US technology companies to spy on dissidents on behalf of foreign governments. NSO Group is an Israeli company founded in 2010 by former members of Israeli intelligence. The company

sells its targeted surveillance product, Pegasus, to multiple intelligence organizations in the Middle East, Europe, and South America. Pegasus enables third-party access to specific mobile devices, without the knowledge or permission of the user of that device, and works to avoid countermeasures aimed at preventing such access, with the ultimate purpose of extracting a wide range of information about (and residing on) that device. NSO Group’s early marketing literature advertised Pegasus as a new “cyber weapon,” which remains the internal conception of their software.¹⁹ However, NSO Group has moved away from this label in recent public communications, instead characterizing their activities as “cyber intelligence.”²⁰

NSO Group operates in a semi-regulated rather than self-regulated space, contending with international agreements such as the Wassenaar Arrangement and domestic law and regulation, and does so openly under the jurisdiction of Israel. Internationally, Israel has agreed to conform to the Wassenaar Arrangement and follow the same human rights conditions as the participating states.²¹ Domestically, Israeli exports are governed under the Import and Export Order of 2006. A draft “Order for Cyber Products Supervision” that appeared to restrict targeted surveillance exports in the manner of the Wassenaar amendments was made public in 2016; however, this did not go beyond the draft stage.²² A lawsuit brought by Amnesty International seeking to withdraw NSO Groups’ export license was rejected by an Israeli court in July 2020,

TABLE 1: Summary of Cases

CASE STUDY	COUNTRY LOCATION	DATES ACTIVE	KEY CUSTOMERS	AAAS PILLARS	US NEXUS
NSO Group	Israel	2016 (first public reports)—present	Worldwide	1-4	Use of US infrastructure
ENFER	Russia	Start date unknown	Russia	1-4	Connection to US adversary
DarkMatter	UAE	2016-present	UAE	1-5	Initially reliant on US expertise

19 Patrick Howell O’Neill, “Inside NSO, Israel’s Billion-Dollar Spyware Giant,” MIT Technology Review, August 19, 2020, <https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/>.

20 NSO Group website, NSO Group, accessed January 24, 2021, www.nsogroup.com.

21 James Shires, *The Politics of Cybersecurity in the Middle East* (London: Hurst Publishers, 2021), www.hurstpublishers.com/book/the-politics-of-cybersecurity-in-the-middle-east.

22 “Israeli Import, Export, Cyber Regulation & Enforcement,” *Shibolet & Co. Law Firm*, May 19, 2020, <https://perma.cc/3WZP-HSHP>.

with the judge pointing to procedures for review based on human rights conditions both before and after sale.²³

NSO Group is thus permitted to operate by the country in which it is based—indeed, it has close connections to Israeli military and intelligence services, like many other cyber companies in Israel (both offensive and defensive).²⁴ Media reports suggest that sellers of these offensive cyber capabilities sometimes bypass the Ministry of Defense, while other times the same companies export specifically for diplomatic purposes (e.g., to strengthen relationships with the Gulf states).²⁵

NSO Group's activities are in the public domain largely due to the investigative work of Citizen Lab, a Canadian research organization based at the University of Toronto. In a 2018 report,²⁶ Citizen Lab identified servers communicating with NSO's Pegasus malware belonging to thirty-six different operators around the world—likely separate security or intelligence agencies. Many operators are in states with poor human rights records and previous indications of targeted surveillance against political opposition, journalists, and dissidents.

A Citizen Lab investigation (the *Million Dollar Dissident* report)²⁷ indicated that Pegasus was used to obtain access to the phone of Emirati activist Ahmed Mansoor in 2016. Later Citizen Lab reports revealed that journalists in Mexico targeted by Pegasus

malware were later killed,²⁸ and that Pegasus may have been tangentially related to the assassination of Saudi journalist Jamal Khashoggi.²⁹ NSO Group software was also discovered on the device of a Catalan independence movement leader in Spain.³⁰ Most recently, Citizen Lab connected NSO's Pegasus malware to the July and August 2020 hack of the personal phones of thirty-six journalists and staff at *Al Jazeera*. These hacks were launched by four Pegasus operators, including SNEAKY KESTRAL and MONARCHY, which are attributed to the United Arab Emirates and Saudi Arabia, respectively.³¹

In 2019, NSO Group reportedly had sixty total customers, with 40 percent in the Middle East, and around \$250 million in revenue in 2018.³² Pegasus sales to the UAE and Saudi Arabia reportedly cost tens of millions of dollars, paid in installments with renewable licenses.³³ NSO Group also works with a range of other companies to deliver more comprehensive surveillance packages. For example, the company has wider links with the UAE, including connections to Emirati cyber-intelligence company DarkMatter.³⁴ NSO Group may also offer other tracking or data analysis products for which there is no public information. For instance, their recent move into coronavirus track-and-trace products in Israel suggests broader capabilities.³⁵

According to open source reporting, NSO Group is the subject of several lawsuits. The highest profile of which is

23 Oded Yaron, "Israeli Court Rejects Request to Revoke Spyware Firm NSO's Export License," *Haaretz*, July 13, 2020, <https://perma.cc/86KT-UECK>.

24 Chaim Levinson, "With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States," *Haaretz.com*, August 23, 2020, <https://perma.cc/VZ84-RS69>.

25 Chaim Levinson, "With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States," *Haaretz*, August 23, 2020, <https://perma.cc/VZ84-RS69>.

26 Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," The Citizen Lab, September 18, 2018, <https://citizenlab.ca/2018/09/hidden-and-see-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.

27 Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Use Against a UAE Human Rights Defender," The Citizen Lab, August 24, 2016, <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>.

28 John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague," The Citizen Lab, November 27, 2018, <https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/>.

29 Bill Marczak et al., *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*, Citizen Lab, October 1, 2018, <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>.

30 Lorenzo Franceschi-Bicchierai and Joseph Cox, "Source: Spain Is Customer of NSO Group," *Motherboard*, July 14, 2020, <https://perma.cc/9MZ3-5SFU>; Stephanie Kirchgaessner and Sam Jones, "Phone of Top Catalan Politician 'Targeted by Government-Grade Spyware,'" *Guardian*, July 13, 2020, <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>.

31 Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert, "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," The Citizen Lab, December 20, 2020, <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-ismessage-zero-click-exploit/>.

32 Becky Peterson and Shayanne Gal, "Leaked Financials Show Israeli Spyware Company NSO Group Is Wildly Profitable despite Concerns over Misuse of Its Technology," *Business Insider*, September 6, 2019, <https://perma.cc/W9AN-229M>.

33 Shires, *The Politics of Cybersecurity in the Middle East*, Chapter Four.

34 See leaked documents available at: Sean Gallagher, "UAE Buys Its Way toward Supremacy in Gulf Cyberwar, Using US and Israeli Experts," *Ars Technica*, February 1, 2019, <https://perma.cc/Q89F-Y6FC>.

35 Joel Schectman, Christopher Bing, and Jack Stubbs, "Special Report: Cyber-Intel Firms Pitch Governments on Spy Tools to Trace Coronavirus," *Reuters*, April 28, 2020, <https://www.reuters.com/article/us-health-coronavirus-spy-specialreport/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus-idUSKCN22A2G1>.

ongoing, brought by WhatsApp in the United States.³⁶ A joint filing of leading technology companies, including Google and Microsoft, for this lawsuit asserted that:

widespread creation and deployment of these tools by private companies acting for profit dramatically increases the risk that these vulnerabilities will be obtained and exploited by malicious actors other than the initial customer to cripple infrastructure, commit large-scale financial crime, or cause other catastrophic damage.³⁷

This move shows that there is significant appetite among leading technology companies for increased regulation in this area.

NSO Group has actively sought to counter allegations of proliferation and abuse via post-sale means, especially through lobbying crucial political circles within the United States. The public disclosure of various lobbying firms working with NSO, including Beacon Global Strategies,³⁸ includes advice on export regulation and promotion of NSO Group's views following negative publicity. More underhand forms of public relations work, including private investigation firms seeking to find compromising information on Citizen Lab, have been attributed to NSO Group in the media, but there is no reliable confirmation of connection.³⁹ Either way, such tactics do not decrease proliferation or abuse risks, they merely affect the perception of NSO Group's responsibility.

Vulnerability research and exploit development

Reporting suggests that NSO Group is active on vulnerability and exploit markets, purchasing multiple high-value vulnerabilities and conducting some in-house research to develop others, though the relative ratio of these activities is unclear. Based on more detailed reporting on NSO Group's competitors, NSO Group likely also has similar long-term supplier relationships with exploit vendors, or cooperates with them in developing exploits.⁴⁰ This means that the distinction between NSO Group's internal activity and that of others on the market is likely not a clear-cut

one: individual researchers that initially sell to NSO Group may later be hired for in-house research, while former NSO Group employees may spin-off their own vulnerability and exploit development companies.⁴¹

Malware payload development

The flagship product of NSO Group, Pegasus, is deployed on target devices through the use of exploits or other methods, like phishing emails. While definitions of payload differ in academic and industry research (and the missile analogy of the word itself is somewhat flawed⁴²), the Pegasus malware is both **multi-stage** and **modular**.⁴³ Multi-stage malware uses several separate exploits, often packaged (and encrypted) separately or in a "dropper." Modular malware has distinct functionalities in logically separate sections, which can either be customized prior to installation or after it is already installed. Developing these payloads is a complex task that is often sidelined in proliferation discussions, and many defense solutions are triggered by subsidiary parts of the malware rather than the exploit itself. Technical analysis of Pegasus indicates significant development in this area as well as the research and development (R&D) above.

Technical command and control (C2)

Pegasus has a sophisticated C2 architecture. Citizen Lab investigations of NSO Group and its competitors relied on internet scanning for fingerprints⁴⁴ of the servers used to communicate with instances of the malware on target devices, as well as those used to host malicious links in 1-click versions. The acquisition of these servers, and their capabilities of avoiding accidental detection or deliberate investigations, is a crucial part of access-as-a-service. Reports suggest that NSO Group generally maintains good operational security in these servers, using decoy pages to reduce suspicion—requiring Citizen Lab to identify undisclosed protocol characteristics (TLS)⁴⁵ that fingerprint NSO Group C2 architecture. Some lapses in operational security have been reported—for example, re-use of domains after the *Million Dollar Dissident* report⁴⁶—but it is unclear whether this was by NSO Group or their customers.

36 Will Cathcart, "Why WhatsApp Is Pushing Back on NSO Group Hacking," *Washington Post*, October 29, 2019, <https://perma.cc/GK33-F35F>.

37 NSO Group v. WhatsApp, (9th Cir. Northern District of California).

38 Josh Rogin, "Washington Must Wake Up to the Abuse of Software that Kills," *Washington Post*, December 12, 2018, <https://www.washingtonpost.com/opinions/2018/12/12/washington-must-wake-up-abuse-software-that-kills/>.

39 Ron Deibert, *Reset: Reclaiming the Internet for Civil Society* (Toronto: House of Anansi, October 6, 2020).

40 Vlad Tsyrlkevich, "Hacking Team: A Zero-Day Market Case Study," Tsyrlkevich.net, July 22, 2015, <https://tsyrlkevich.net/2015/07/22/hacking-team-0day-market/>.

41 O'Neill, "Inside NSO, Israel's Billion-Dollar Spyware Giant."

42 While missile payloads refer to the explosive warhead, a malware payload is the portion of the malware which performs malicious action. However, unlike a warhead which has a single function (to explode), malware payloads can include backdoors that can also drop additional payloads. In this sense, payloads can be delivery mechanisms for other payloads or even other exploits.

43 Ben Buchanan, "The Legend of Sophistication in Cyber Operations," Belfer Center Cyber Security Project, January 2017, <https://www.belfercenter.org/sites/default/files/files/publication/Legend%20Sophistication%20-%20web.pdf>.

44 Marczak, Scott-Railton, McKune, Razzak, and Deibert, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries."

45 Ibid.

46 Marczak and Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Use Against a UAE Human Rights Defender."

Operational management

This is the pillar that NSO Group engages in least, according to public reporting. The company's statements consistently indicate that NSO Group does not make decisions about who to target, and this is supported by public information about targets; indeed, the term "Access-as-a-Service" implies this is perhaps the only remaining decision required by the service's user. When it comes to command and control during an operation, the company insists it does not conduct any operations whatsoever. Whether it does in reality is difficult to know definitively for several reasons, including the semantics of what "conducting operations" entails (but whether it means providing support while an operation is in progress or providing the infrastructure for operations qualifies, NSO does both). But their unavoidable involvement, especially insofar as the nature of the malware and the infrastructure used, is, at the very least, a risk in terms of being blamed for operations by incident investigators. The other aspects of this pillar, especially the strategic organization of resources and teams, may well be satisfied by NSO Group. Leaked documents suggest they work closely with other companies providing complementary capabilities to clients, and it is unclear what influence they have in this process.⁴⁷

Training and support

NSO Group provides extensive training and support to its clients. This ranges from initial demonstrations of its technology, reportedly tailored to target devices selected by the client, to training on its use by client operators and ongoing on-site support with engineers, troubleshooting and resolving technical problems with the software as they arise.

2. ENFER

Introduction and background

ENFER is the cryptonym we have chosen for a Russian cybersecurity services provider assisting the Russian intelligence services with its offensive cyber operations, building up capabilities that Russia may decide to use against strategic adversaries. It is active within the Russian marketplace and across a number of global offices, which

publicly offers code audit, penetration testing and threat emulation, vulnerability discovery and management, threat detection and remediation, and threat intelligence services for corporate and government customers, along with associated training services. The firm has acknowledged the Ministry of Defense of the Russian Federation as one of their first clients, having officially formed a relationship within the first two years of the company's founding. This relationship was further strengthened by unspecified cooperation with security services over the past decade.⁴⁸ Through discussions under the Chatham House rule with various sources, the authors of this report determined that the tactics of this actor are noteworthy enough to be published here.

ENFER staff and other Russian cybersecurity professionals have described the company's activities as providing a platform for capabilities development and access. The firm reportedly develops and supports offensive cyber capabilities and operations for multiple clients. This allegedly encompasses work in response to direct tasking by officers of the FSB on specific projects involving offensive activities, including exploit discovery and weaponization, malware development, and infrastructure engineering.⁴⁹ Like NSO Group, ENFER operates in a semi-regulated rather than self-regulated space, is permitted to operate by the country in which it is based, and exists in the same space as international agreements, domestic law, and regulation.

Vulnerability research and exploit development

ENFER conducts unique vulnerability discovery research and further engineering to develop reliably weaponized exploit code targeting these vulnerabilities. These Oday vulnerabilities are described as intended for use in penetration testing engagements and other red team offensive security activities.⁵⁰ However, these capabilities are also provided to Russian government clients and a selected subset of these exploits have also been publicly disclosed through security community channels. Such limited disclosures have allegedly been driven by apparent intent to deny capabilities to offensive cyber programs outside of Russia, where vulnerabilities are believed to be actively exploited or under threat of bug collision.⁵¹

47 Gallagher, "UAE Buys Its Way toward Supremacy in Gulf Cyberwar, Using US and Israeli Experts"; and Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," The Citizen Lab, December 1, 2020, <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>.

48 ENFER corporate history document, 2018.

49 Discussion with authors under Chatham House rule restrictions, July 12, 2020.

50 Ibid.

51 Discussion with authors under Chatham House rule restrictions, August 19, 2020. For more on collisions, see: Lillian Ablon and Andy Bogart, "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," RAND Corporation, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf; and Trey Herr, Bruce Schneier, and Christopher Morris, "Taking Stock: Estimating Vulnerability Rediscovery," Belfer Center Cyber Security Project, October 2017, https://www.schneier.com/wp-content/uploads/2017/03/Vulnerability_Rediscovery.pdf.

ENFER has also reportedly been involved in reverse engineering and parallel redevelopment of new capabilities based on samples captured in the wild, particularly involving unique payloads recovered from Russian government networks.⁵² In at least one case, this allegedly involved a malware family attributed by Russian researchers to the alleged cyber operations of a Five Eyes member state, delivered through a then unknown Oday exploit in a campaign detected between 2014 and 2015. The captured exploit in this case was reportedly repurposed by ENFER for use in other intrusions, stripped of the countermeasures that would prevent subsequent additional reuse.⁵³

Similar exploit capture and replay has been alleged in cases involving Chinese-attributed intrusion sets, where the BUCKEYE (also known as APT3, GOTHIC PANDA, or BORON) intrusion set deployed exploit code targeting the Microsoft Windows CVE-2017-0143 vulnerability to deliver a variant of the DOUBLEPULSAR malware family in early 2016. Both this vulnerability and the associated implant would subsequently be identified in a collection of purported US government offensive tooling publicly released by the ShadowBrokers in 2017.⁵⁴ It is significant that Western cybersecurity researchers and the US government have attributed the APT3 / GOTHIC PANDA intrusion set to Boyusec, a Guangzhou-based contractor to the Chinese Ministry of State Security intelligence service.⁵⁵ Boyusec also allegedly provided a platform for offensive cyber capabilities and access in a relatively similar model to ENFER (albeit with some structural differences that may be attributed to different service operational practices).⁵⁶

Malware payload development

ENFER is reported to have developed multiple malware payload variants for offensive use, including systems reconnaissance and document exfiltration, for the FSB.⁵⁷ This relationship is consistent with other interactions between

the FSB and its contractors, including InformInvestGroup CJSC and ODT LLC. These entities developed the FRONTON malware family, intended to compromise vulnerable internet of things (IoT) devices in order to provide offensive cyber capabilities for distributed denial of service (DDOS) attacks, likely as well as additional utility as proxy infrastructure. The FSB 2nd Directorate, Information Security Center (also known as Center 18, or under unit cover designator 64829), was identified as the ultimate customer for this capability. Documentation of this acquisition was made public following the compromise of contractor networks by a previously unknown, ideologically motivated hacktivist organization calling itself Digital Revolution.⁵⁸

More significant and unique capabilities were provided that focused on Signaling System 7 (SS7) telecommunications networks. Exploitation scenarios involving vulnerable telephony signaling transport protocols had been known to the global research community for some time, following theoretical discussions involving major industry stakeholders.⁵⁹ The offensive research community had also explored practical applications of these techniques at public hacker conference presentations and in commercial penetration testing engagements.⁶⁰ However, this starting point led to options that were further matured based on ENFER's extensive experience with a prominent Russian telecommunication client where the firm had initially been separately contracted to provide defensive cybersecurity assessment services.⁶¹ Offensive cyber capabilities developed over this period reportedly included not only geolocation and denial of service options abusing poorly secured administrative functions inherent to the SS7 protocol but also intercept and implant delivery through man-in-the-middle techniques. Implants allegedly were tailored for older generation Android devices, having been created in part through redevelopment of then-available commodity criminal malware tooling.⁶²

52 Discussion with authors under Chatham House rule restrictions August 19, 2020.

53 Discussion with authors under Chatham House rule restrictions, July 12, 2020.

54 "Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak," Symantec, May 6, 2019, <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit>.

55 "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," US Department of Justice, November 27, 2017, <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations#:~:text=November%2027%2C%202017-.U.S.%20Charges%20Three%20Chinese%20Hackers%20Who%20Work%20at%20Internet%20Security,Three%20Corporations%20for%20Commercial%20Advantage&text=Boente%2C%20Acting%20U.S.%20Attorney%20Soo,Pittsburgh%20Division%20announced%20the%20charges.>

56 "The Destruction of APT3," Intrusion Truth, May 22, 2018, <https://intrusiontruth.wordpress.com/2018/05/22/the-destruction-of-apt3/>.

57 Discussion with authors under Chatham House rule restrictions, July 12, 2020

58 Catalin Cimpanu, "Hackers breach FSB contractor and leak details about IoT hacking project," ZDNet, March 20, 2020, <https://www.zdnet.com/article/hackers-breach-fsb-contractor-and-leak-details-about-iot-hacking-project/>.

59 J. Loughney, M. Tuexen, and J. Pastor-Balbas, "RFC3788: Security Considerations for Signaling Transport (SIGTRAN) Protocols," Network Working Group, Internet Engineering Task Force, June 2004, <https://datatracker.ietf.org/doc/rfc3788/>.

60 Philippe Langlois, "Toward the HLR, attacking the SS7 & SIGTRAN applications," Hackers to Hackers Conference (H2HC) (Sao Paulo, November 2009): 28-29; Laurent Ghigonis, "Hacking Telco Equipment: The HLR/HSS," Hackito Ergo Summit (Paris, April, 2014): 24-26; and Laurent Ghigonis & Alexandre de Oliveira, "SS7map: Mapping Vulnerability of the International Mobile Roaming Infrastructure," Chaos Communication Congress, (Hamburg, December 2014): 27-30.

61 Discussion with authors under Chatham House rule restrictions, July 12, 2020.

62 Discussion with authors under Chatham House rule restrictions, December 9, 2020.

These capabilities would reportedly be further deployed within networks operated by the firm's international telecommunications sector clients, and deployment expanded to include operations across the Middle East on behalf of other state services. Again, ENFER's initial activities would be characterized as defensive in nature, involving penetration testing and other security assessment purposes. These engagements often closely followed similar assessments conducted by Western firms with other regional peer telecom organizations, further providing a veneer of legitimacy to ENFER. However, identified vulnerabilities found in regional telecom networks were also reportedly exploited for operational objectives associated with ongoing espionage.⁶³

Technical command and control

ENFER operators have reportedly been directly involved in systems administration, and interactive command and control, of deployed intrusion access capabilities.⁶⁴ In particular, ENFER staff are purported to have been critical to actions abroad where FSB officers were not operating directly onsite at other firms.

Operational management

The extent to which ENFER staff have been involved in the planning and management of operations remains unclear. In multiple instances, ENFER staff may have been involved in operations not performed at the direction of a state.⁶⁵ Such corruption has been previously noted in major cases involving FSB officers and contractors associated with the cyber mission, including with the previously mentioned Center 18.⁶⁶ In late 2016, multiple FSB officers and a contractor working for a different cybersecurity firm were arrested on complex charges that included allegations of personal unjust enrichment due to involvement in cybercrime activities

dating back to at least 2004. The details of the subsequent convictions remain unclear, in part due to additional charges of treason based on supposed cooperation with foreign intelligence services, but described fact patterns included deployment of specific malware implants outside of officially contemplated scenarios and attempts to acquire access to confidential business information held by private financial institutions.⁶⁷ These allegations mirror US Department of Justice (DOJ) indictments that named several of the involved individuals in connection with the compromise of a prominent US technology firm in a 2014 campaign.⁶⁸

Some FSB oversight of ENFER staff has been noted, but appears to be focused in the context of counterintelligence review. These mechanisms also reportedly focus on informal coercion—including threats against individual staffers' families. This is consistent with reporting in other instances where the FSB has sought to leverage family relationships as a source of pressure on persons recruited for clandestine activities in order to motivate continued involvement, rather than a mechanism to ensure responsible, professional behavior.⁶⁹

Training and support

ENFER provides multiple training services across Russian and other government clients, as well as for private sector entities.⁷⁰ Many of these training activities are inherently dual-use in nature, and are easily focused on purely offensive objectives. The multi-participant nature of many of the events also provides opportunities for Russian intelligence officers to spot, assess, and develop potential targets for future espionage, including cultivation of prospective assets for recruitment approaches. Specific, apparently requirement-driven, elicitation has also been described by foreign cybersecurity professionals attending these events.⁷¹

63 Ibid.

64 Discussion with authors under Chatham House rule restrictions, July 12, 2020.

65 Ibid.

66 "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," US Department of Justice, March 15, 2017, <https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions>.

67 Kimberly Zenz, "Infighting Among Russian Security Services in the Cyber Sphere," Black Hat USA, August 3–8, 2018, <https://i.blackhat.com/USA-19/Thursday/us-19-Zenz-Infighting-Among-Russian-Security-Services-in-the-Cyber-Sphere.pdf>; and "String of Baffling Arrests Shakes Cyber Division of FSB," Recorded Future, January 27, 2017, <https://www.recordedfuture.com/russian-cyber-arrests/>.

68 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, (Cambridge: Cambridge University Press, 2018).

69 "Spies Without Borders - How the FSB Infiltrated the International Visa System," Bellingcat, November 16, 2018, <https://www.bellingcat.com/news/uk-and-europe/2018/11/16/spies-without-borders-fsb-infiltrated-international-visa-system/>.

70 Company promotional material, circulated June 2018.

71 Discussion with authors under Chatham House rule restrictions, December 2, 2018.

3. DARKMATTER GROUP

Introduction and background

DarkMatter Group (also known as DarkMatter LLC or simply “DarkMatter”) is a cyber security company based in the United Arab Emirates. Initially set up by US government contractors to help the UAE develop cyber capabilities, the firm has now conducted operations against US citizens and recruits western security researchers to further its espionage capabilities. According to interviews with UAE officials, DarkMatter allegedly acts as a way to sidestep the Wassenaar Arrangement—if Western offensive security vendors are limited by export controls, building a native cyber security vendor made up of foreign talent circumvents the arrangement while building government-backed capabilities.⁷² According to open-source reporting, DarkMatter is also closely involved in operational targeting decisions.⁷³

The United Arab Emirates is a heavily targeted country for cyberattacks, especially within their oil and gas sectors.⁷⁴ The country’s national offensive cyber capabilities were limited until 2008, when former US counter-terrorism coordinator Richard Clarke helped create and mature the UAE’s first cyber surveillance agency through his own company, Good Harbor Consulting. In 2010, the UAE moved to further supplement their cyber capabilities through other contractors, like US firm Cyberpoint,⁷⁵ whose notorious Project Raven taught US espionage tactics to UAE operatives.⁷⁶ The American contingent of Project Raven, made up primarily of former

US intelligence officers, identified vulnerabilities in targets, developed or acquired malware for the targets, and assisted the Emiratis in conducting operations.⁷⁷

In 2016, the Emirati government moved oversight of Project Raven to DarkMatter,⁷⁸ multiple Cyberpoint employees left their company to work for DarkMatter,⁷⁹ and targeting within Project Raven began to expand to US citizens under the company’s watch.⁸⁰ According to experts, DarkMatter is intrinsically linked to the UAE’s national intelligence agencies, like the National Electronic Security Authority (NESA) (now called the Signals Intelligence Agency), the UAE’s National Security Agency (NSA) equivalent.⁸¹ Like NSO Group and ENFER, DarkMatter operates in a semi-regulated rather than self-regulated space, allegedly operating at the behest of the UAE government.

DarkMatter Group advertises four separate services:⁸² a digital and applied technology arm (named DigitalX1)⁸³ that claims to assist businesses and governments with harnessing advanced technologies, an education arm (DigitalE1)⁸⁴ providing a digital talent pool to embed within company clients, government services dedicated to helping governments “strengthen their defense and security posture through bespoke technologies,”⁸⁵ and their namesake Cyber Security and Secure Communications practice (DarkMatter) focusing on security, safety, and resilience for businesses. The company primarily works for the Emirati government and related entities.⁸⁶

72 Michael Sexton and Eliza Campbell, *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization* (Washington, DC: Middle East Institute, October 2020).

73 Christopher Bing and Joel Schectman, “Inside the UAE’s Secret Hacking Team of American Mercenaries,” Reuters, January 20, 2019, <https://www.reuters.com/investigates/special-report/usa-spying-raven/> This states that targets were provided by UAE officials, but that these officials worked together with employees in a single building, all within DarkMatter. “Under DarkMatter, Project Raven continued to operate in Abu Dhabi from the Villa, but pressure escalated for the program to become more aggressive. Before long, senior NESA officers were given more control over daily functions, former Raven operatives said.” The involvement of DarkMatter in targeting decisions stems from the integration of NESA staff into the company.

74 Weizhen Tan, “Cyberattacks in the Middle East Are on the Rise: Here’s Who They’re Targeting,” *CNBC*, June 18, 2019, <https://www.cnbc.com/2019/06/18/cyberattacks-in-uae-middle-east-darkmatter-report.html>.

75 Joel Schectman and Christopher Bing, “Special Report: White House Veterans Helped Gulf Monarchy Build Secret Surveillance Unit,” Reuters, December 10, 2019, <https://www.reuters.com/article/us-usa-raven-whitehouse-specialreport/special-report-white-house-veterans-helped-gulf-monarchy-build-secret-surveillance-unit-idUSKBN1YE10B>.

76 Bing and Schectman, “Inside the UAE’s Secret Hacking Team of American Mercenaries.”

77 Ibid.

78 Ibid.

79 Jenna McLaughlin, “How the UAE is Recruiting Hackers to Create the Perfect Surveillance State,” *The Intercept*, October 24, 2016, <https://theintercept.com/2016/10/24/darkmatter-united-arab-emirates-spies-for-hire/>.

80 Bing and Schectman, “Inside the UAE’s Secret Hacking Team of American Mercenaries.”

81 Sexton and Campbell, *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*.

82 “Dark Matter,” VMware Carbon Black, accessed January 24, 2021, <https://www.carbonblack.com/partner/dark-matter/>; and “Dark Matter,” LinkedIn, accessed January 24, 2021, <https://www.linkedin.com/company/dark-matter-llc/about/>.

83 “DarkMatter Group Calls for Improved Vigilance as UAE’s Cyber-Threat Landscape Reaches Critical Level,” CISION PR Newswire, June 17, 2019, <https://www.prnewswire.com/ae/news-releases/darkmatter-group-calls-for-improved-vigilance-as-uae-s-cyber-threat-landscape-reaches-critical-level-881538662.html>.

84 Ibid.

85 Ibid.

86 Alexander Cornwell, “Emerging Gulf State Cyber Security Powerhouse Growing Rapidly in Size, Revenue,” Reuters, February 1, 2018, <https://www.reuters.com/article/us-emirates-cyber-darkmatter/emerging-gulf-state-cyber-security-powerhouse-growing-rapidly-in-size-revenue-idUSKBN1FL451>.

DarkMatter has released the KATIM secure smartphone as a purely defensive product⁸⁷ and produced multiple threat intelligence reports⁸⁸ (once ironically calling out a separate potential cyber mercenary firm⁸⁹), but it is best known for its connections to UAE state-sponsored cyberattacks against dissidents both within the UAE's borders and worldwide. Public claims of DarkMatter exploiting vulnerabilities and deploying malware for surveillance purposes against Emirati citizens first emerged in 2016, when DarkMatter allegedly attempted to recruit an Italian security researcher, as well as at least five other foreign cyber security researchers,⁹⁰ although this number may not reflect the full extent of the security researcher targets. According to Reuters, current and former DarkMatter employees are being investigated by the US Federal Bureau of Investigation (FBI) regarding the transfer of classified US surveillance techniques under Project Raven.⁹¹ DarkMatter's founder has claimed that DarkMatter has "no depository of zero day exploits," and does not take part in "offensive hacking" operations.⁹² However, the close ties of the company to the Emirati government, its continuation of Project Raven, and its connection to Totok—an Emirati messaging app⁹³—suggest otherwise. Multiple former DarkMatter employees have claimed that the company has targeted reporters and human rights activists, including Canadian research organization CitizenLab.⁹⁴

Vulnerability research and exploit development

DarkMatter is reported to buy exploits from other vendors, in addition to discovering vulnerabilities to exploit in-house.⁹⁵ Given DarkMatter's link to Project Raven, and

heavy recruitment efforts to bring in offensive security researchers, including those engaged in automobile vulnerability research,⁹⁶ DarkMatter likely has native vulnerability research talent within the company. As for DarkMatter's exploit procurement process, one public data point alluding to DarkMatter's vendor connections emerged in 2019 when *Vice News* reporter Joseph Cox claimed he had been contacted by a representative from Saudi offensive security company Haboob. The representative allegedly reached out to purchase Oday vulnerabilities from Cox "for both offensive and defensive purposes,"⁹⁷ not realizing that Cox was a journalist. According to Cox's article, multiple outside sources have claimed that DarkMatter and Haboob are connected.

Malware payload development

While not linked to any offensive security product, DarkMatter has been linked to a chat application that surreptitiously provided user information to the Emirati government. Totok was the name of a mobile application used by the Emirati government in 2019 to collect conversations, locations, contacts, calendars, and other phone data from unsuspecting victims.⁹⁸ The company behind the application, Breej Holding, was linked to DarkMatter by multiple security researchers. While Totok did not weaponize any vulnerabilities and had legitimate chat functionality, the chat app can be classified as malware connected to DarkMatter due to the amount of personal information taken without proper disclosure and user consent.⁹⁹ A majority of Totok's users were located in the UAE, but the app also boasted a large number of US and

87 "DarkMatter Group Unveils World's First Ultra Secure Smartphone for Extreme Field Conditions," CISION PR Newswire, February 27, 2019, <https://www.prnewswire.com/ae/news-releases/darkmatter-group-unveils-worlds-first-ultra-secure-smartphone-for-extreme-field-conditions-300803058.html>.

88 "DarkMatter Group Calls for Improved Vigilance as UAE's Cyber-Threat Landscape Reaches Critical Level," CISION PR Newswire.

89 Hack in the Box Security Conference, "#HITBGSEC 2018 COMMSEC: The Trails Of WINDSHIFT APT - Taha Karim," YouTube video, 55:19, September 16, 2018, https://www.youtube.com/watch?v=KEJn7qSOaXo&ab_channel=HackInTheBoxSecurityConference.

90 Jenna McLaughlin, "How the UAE Recruited Hackers to Create the Perfect Surveillance State"; "DarkMatter to Lead the Region in Certification Authority Services with Appointment of PKI Specialist," CISION PR Newswire, March 29, 2016, <https://www.prnewswire.com/news-releases/darkmatter-to-lead-the-region-in-certification-authority-services-with-appointment-of-pki-specialist-573814631.html>.

91 Bing and Schectman, "Inside the UAE's Secret Hacking Team of American Mercenaries"; and Mark Mazzetti, Adam Goldman, Ronen Bergman, and Nicole Perloth, "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments," *New York Times*, March 21, 2019, <https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html>.

92 Jon Gambrell, "UAE Cyber Firm DarkMatter Slowly Steps Out of the Shadows," AP News, February 1, 2018, <https://apnews.com/article/e6c2cb4445b5464b8b9548f7d314e9b8>.

93 Mark Mazzetti, Nicole Perloth, and Ronen Bergman, "It Seemed Like a Popular Chat App, It's Secretly a Spy Tool," *New York Times*, August 14, 2020, <https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html>.

94 Mark Mazzetti, Adam Goldman, Ronen Bergman, and Nicole Perloth, "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments," *New York Times*, March 21, 2019, <https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html>.

95 Shires, *The Politics of Cybersecurity in the Middle East*, Chapter Four.

96 Jenna McLaughlin, "How the UAE is Recruiting Hackers to Create the Perfect Surveillance State."

97 Joseph Cox, "A Saudi Cybersecurity Company Tried to Buy Zero Day Exploits from Me," *Vice*, March 12, 2019, <https://www.vice.com/en/article/xwbk5j/saudi-cybersecurity-company-tried-buy-zero-days-from-me-haboob-darkmatter>.

98 Mazzette, Perloth, and Bergman, "It Seemed Like a Popular Chat App. It's Secretly a Spy Tool."

99 "Malware Categories," Google Play Protect, accessed January 24, 2021, <https://developers.google.com/android/play-protect/phacategories>.

international users, totaling five million Android downloads alone by the time it was removed from the Google Play store.¹⁰⁰

Technical command and control

Project Raven, prior to and likely after evolving into DarkMatter, contained an infrastructure department that used anonymous identities and Bitcoin to set up untraceable command and control servers for their operations. Around the same time the project moved to DarkMatter, CitizenLab released a report on DarkMatter's operations (under the threat actor name "Stealth Falcon").¹⁰¹ According to the report, Stealth Falcon used phishing emails containing a shortened link to fingerprint a target's browser and antivirus prior to downloading malware onto the target's machine.¹⁰²

DarkMatter has also made serious attempts to become a certificate authority, only to have its requests denied.¹⁰³ Certificate authorities are a select few organizations that issue digital certificates to websites, software, and other entities, verifying that a website or software is from a trusted party.¹⁰⁴ Once Project Raven became public knowledge, Mozilla and Google blocked DarkMatter's attempt at becoming a certificate authority.¹⁰⁵ Had DarkMatter become a certificate authority, any offensive security operations the company undertook could take advantage of its certificate authority status to mask its technical command and control domains as legitimate websites¹⁰⁶ and trick unsuspecting victims into downloading seemingly legitimate software, only to infect the victim with malware.

Operational management

DarkMatter's historical operational management structure is well documented.¹⁰⁷ The UAE government allegedly tasked Project Raven with a list of targets. Cyberpoint's American

employees then identified vulnerabilities in the targets, developed or purchased intrusion software, and assisted in monitoring, while Emirati operatives carried out the actual operation. After Project Raven evolved into DarkMatter, the company altered operational management such that Emiratis were conducting operations against US citizens without the awareness of DarkMatter's American employees.

DarkMatter's operational management processes have remained similar to those observed in Project Raven for at least one of their primary clients, the UAE Signals Intelligence Agency. According to public reporting on sources within the company, any media report of DarkMatter instantly warranted a "tiger team," or specialized response group, of company employees who would create lists of individuals related to the report for future targeting.¹⁰⁸ This is reminiscent of Project Raven's original targeting division, which would monitor the internet for mentions of DarkMatter to ensure that the company's name was not attached to offensive operations being done on behalf of the UAE.¹⁰⁹

Training and support

DarkMatter has provided open courses to industry professionals on "Offensive Mobile Penetration Testing and Reversing" at prominent cyber security conference BlackHat.¹¹⁰ The company also provides training and support to clients through advertised core services. Its education arm (DigitalE1)¹¹¹ provides a digital talent pool to embed its employees within company clients. As DarkMatter aggressively hires international talent, including offensive security talent from US¹¹² and Israeli¹¹³ intelligence agencies, it is possible that some of these individuals may directly support corporations or governments in the Middle East.

100 Mazzette, Perloth, and Bergman, "It Seemed Like a Popular Chat App. It's Secretly a Spy Tool."

101 Bill Marczak and John Scott-Railton, "Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents," The Citizen Lab, May 29, 2016, <https://citizenlab.ca/2016/05/stealth-falcon/>.

102 Ibid.

103 "DarkMatter to Lead the Region in Certification Authority Services With Appointment of PKI Specialist," CISION PR Newswire; and Joel Schectman and Christopher Bing, "Mozilla Blocks UAE Bid to Become an Internet Security Guardian After Hacking Reports," Reuters, July 9, 2019, <https://www.reuters.com/article/us-usa-cyber-mozilla/mozilla-blocks-uae-bid-to-become-an-internet-security-guardian-after-hacking-reports-idUSKCN1U42CA>.

104 Casey Crane, "What is a Certificate Authority (CA) and What Do They Do?," Security Boulevard, August 11, 2020, <https://securityboulevard.com/2020/08/what-is-a-certificate-authority-ca-and-what-do-they-do/>.

105 Schectman and Bing, "Mozilla Blocks UAE Bid to Become an Internet Security Guardian After Hacking Reports."

106 "HTTPS Spoofing," The Secret Security Wiki, accessed January 24, 2021, <https://doubleoctopus.com/security-wiki/threats-and-tools/https-spoofing/>.

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

108 Sam Biddle and Matthew Cole, "Team of American Hackers and Emirati Spies Discussed Attacking the Intercept," The Intercept, June 12, 2019, <https://theintercept.com/2019/06/12/darkmatter-uae-hack-intercept/>.

109 Ibid.

110 "Offensive Mobile Exploitation & Reversing," Black Hat USA 2018, accessed January 24, 2021, <https://www.blackhat.com/us-18/training/offensive-mobile-exploitation-and-reversing.html>.

111 Ibid.

112 Jenna McLaughlin, "How the UAE is Recruiting Hackers to Create the Perfect Surveillance State."

113 "UAE-Based Intelligence Firm said Recruiting IDF Veterans from Elite Cyber Unit," *Times of Israel*, October 18, 2019, <https://www.timesofisrael.com/uae-based-intelligence-firm-said-recruiting-idf-veterans-from-elite-cyber-unit/>.

Previous approaches to countering proliferation of OCC

The question of who can build, sell, and use OCC and the role that states should play in restricting any of these activities has been the subject of intense debate for more than a decade.¹¹⁴ Countering the proliferation of these capabilities is an active area of policy innovation, but it is hamstrung by ideological schisms and poor understanding of the dynamics of proliferation. One group's repressive surveillance regime is another's legitimate national security activity.¹¹⁵ Consequently, efforts to prevent human rights violations facilitated by OCC often run aground in the strong tides of commercial and geopolitical incentives to share such capabilities. More broadly, attempts to share OCC between allies without allowing their runaway spread and to better limit the diffusion of human talent from top-flight intelligence organizations raises fundamental national security questions, alongside issues of human rights and individual misuse.

And so lines are drawn, and blurred, and drawn again in a contest of research and rhetoric. The result is at least one serious international effort¹¹⁶ at state-level restrictions in the Wassenaar Arrangement, although its limitations, controversy, and resulting uneven implementation do not make it a model for imitation. Offensive cyber capabilities continue to spread,

and cyberattacks that utilize these capabilities—ranging from surveillance and espionage operations to destructive attacks on critical infrastructure—continue unabated.

The two most frequently discussed tools within counter-proliferation circles are international law and norms on the one hand, and deterrence on the other. However, these both fall short when tackling OCC proliferation at the corporate level through AaaS. First, many cybersecurity norms have been pushed actively by the international community,¹¹⁷ but often fail to influence domestic law and policy.¹¹⁸ Broad international agreements might offer strong levers of policy coordination but domestic policies would need to accurately and effectively specify the activities to be curtailed, something which appears to be missing from almost every computer crime statute.¹¹⁹ Furthermore, domestic law, and thus law enforcement, struggle to keep pace with emerging cyber security threats, let alone the supply chain behind them.¹²⁰ In areas where many actors are capable of breaking a norm or law and enforcement is inconsistent or non-existent, norms and laws have limited potential. So far, they have had little impact on slowing cybercrime, plausibly deniable behaviors like election interference, or the activities examined in this report's case studies.

-
- 114 Herbert Lin, "Arms Control in Cyberspace: Challenges and Opportunities," *World Politics Review*, March 6, 2012, <http://www.worldpoliticsreview.com/articles/11683/arms-control-in-cyberspace-challenges-and-opportunities>; Ron J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Plattsburgh, NY: Signal Books, 2013), <https://blackcodebook.com/#:~:text=In%20Black%20Code%2C%20Ronald%20J,agents%20are%20scrambling%20for%20control>; Tim Stevens, "Cyberweapons: Power and the Governance of the Invisible," *International Politics* 55, no. 3 (May 1, 2018): 482–502, <https://link.springer.com/article/10.1057/s41311-017-0088-y>; Jon Randall Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Digital Policy, Regulation and Governance* 19, no. 6 (January 1, 2017): 493–514, <https://www.emerald.com/insight/content/doi/10.1108/DPRG-05-2017-0023/full/html>; and Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* (March 4, 2020): 1–34, <https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354>.
- 115 James Shires, "Family Resemblance or Family Argument? Three Perspectives of Cybersecurity and Their Interaction," *St Anthony's International Review* 14, no. 3 (2019): 18–36, <https://www.ingentaconnect.com/content/stair/stair/2019/00000015/00000001/art00003>.
- 116 Jukka Ruohonen and Kai K. Kimppa, "Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity," *Journal of Information Technology & Politics* (2019), <https://arxiv.org/pdf/1906.02235.pdf>.
- 117 Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer, "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads," Carnegie Endowment for International Peace, February 26, 2020, <https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110>.
- 118 Dan Ward and Robert Morgus, Professor Cy Burr's Graphic Guide to: International Cyber Norms," New America Cybersecurity Initiative, November 2016, <https://na-production.s3.amazonaws.com/documents/CyberNorms114.pdf>.
- 119 "Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime," Council of Europe, January 7, 2004, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=RckTQL9k; James Shires, "Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf," in *Governing Cyberspace: Power, Behavior, and Diplomacy*, eds. Dennis Broeders and Bibi van den Berg (London: Rowman & Littlefield Publishers, Inc., 2020), 205–26.
- 120 Josephine Wolff, "The New Economics of Cybercrime," *the Atlantic*, June 7, 2016, <https://www.theatlantic.com/business/archive/2016/06/ransomware-new-economics-cybercrime/485888/>; Kurt Thomas, Danny Yuxing Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J. Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna, "Framing Dependencies Introduced by Underground Commoditization," accessed January 24, 2021, <http://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43798.pdf>; and Keman Huang, Michael Siegal, and Stuart Madnick, "Systematically Understanding the Cyber Attack Business: A Survey," MIT Cybersecurity Interdisciplinary Systems Laboratory, July 2018, <http://web.mit.edu/smadnick/www/wp/2018-08.pdf>.

Second, for the better part of a century, international relations scholars have offered differing definitions and debated the core tenets of deterrence.¹²¹ Deterrence is most effective in shaping behavior when the deterring actor is able to offer a credible threat of retaliation for a given behavior, and when the target of the deterrence both understands the threat and wishes to avoid it. Signaling is important—deterrence and compellence have utility when the actors involved successfully signal their commitment to these strategies. Behind the hazy veil of state/proxy relationships, and even in legitimate commercial business transactions, however, this commitment is as limited in its perception as it is in practice. Complete deterrence is challenging, due in part to the nature of the domain and the multitude of actors with diverse decision-making strategies. Partial deterrence is not impossible however. Deterrence, as a component of a larger strategy, can use the levers of economics, diplomacy, military, politics, and information to reduce the benefit malicious actors reap in attacking entities in the United States and its allies.¹²²

There are recommendations from within the cybersecurity community as well, though they generally fail to address all

five pillars of cyber capability or proliferation directly. Generally, improving cyber defense is a broad but essential part of limiting the impact of AaaS. Within the cyber policy community, a few notable recommendations have been made to counter proliferation of OCC that are far more specific. Incentivizing government and private sector bug bounty programs, encouraging domestic security research, and creating more government job incentives for cyber roles are all good concepts, but do not actively target proliferation emerging from private companies themselves, and are not within the scope of this paper.¹²³ Shortening the vulnerability identification and mitigation cycle on a large scale while targeting the most widely impactful software flaws could be beneficial, but only for the Vulnerability Research and Exploit Development cyber capabilities pillar.¹²⁴ One sagacious member of the technology and security communities suggested the United States might simply outbid all potential customers for vulnerabilities on the regulated and semi-regulated markets, cornering the market on known flaws and widely expanding the ranks of those hunting for them.¹²⁵ This works as a useful thought experiment, illustrating deficiencies in how the marketplace allocates risk from insecure software, though it would present difficulties as a practical policy measure.

121 Lawrence Freedman, "Does Deterrence Have a Future," Arms Control Association, October, 2000, <https://www.armscontrol.org/act/2000-10/features/does-deterrence-future>; Alexander L. George and Richard Smoke, "Deterrence in American Foreign Policy," *World Politics* 41, no.2 (January, 1989): 170-182, <https://doi.org/10.2307/2010406>; Thomas C. Schelling, *Arms and Influence* (London: Yale University Press, November 5, 2008), <https://yalebooks.yale.edu/book/9780300143379/arms-and-influence>; Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44-71, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266.

122 Matthew Kroenig and Barry Pavel, "How to Deter Terrorism," *The Washington Quarterly* 35, no. 2 (Spring 2012): 21-36, <https://doi.org/10.1080/0163660X.2012.665339>.






123 Andreas Kuehn and Ryan Ellis, "Bug Bounty Programs: Institutional Variation and the Different Meanings of Security," in *Rewired: Cybersecurity Governance*, eds. Ryan Ellis and Vivek Mohan (Hoboken: Wiley, April 25, 2019).

124 Trey Herr, "Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle."

125 Dan Geer, "Cybersecurity as Realpolitik," August 6, 2014, <http://geer.tinho.net/geer:blackhat.6viii14.txt>.

Countering Proliferation Policy Recommendations

TABLE 2: Summary of Policy Recommendations

		PILLARS				
		1	2	3	4	5
 1 Vulnerability research and exploit development						
 2 Malware payload development						
 3 Technical command and control						
 4 Operational management						
 5 Training and support						
Understand and partner	Build a coalition of like-minded partners				●	
	Elevate the issue of offensive cybersecurity capabilities proliferation in international forums.				●	
	Pass “Know Your Vendor” laws or regulations.	●		●	●	
Shape	Develop ban lists for vendors that are caught selling capabilities to states or entities on published lists of concern.		●		●	●
	Standardize risk assessment for the Access-as-a-Service industry.		●		●	●
	Incentivize corporate ethics committees.				●	●
	Limit foreign military sales and other foreign assistance to states that purchase from banned AaaS providers or use AaaS tools to infringe on human rights.				●	
Limit	Widen the scope of selective defensive vulnerability disclosure.	●	●	●		
	Establish post-employment restrictions for former government cybersecurity employees.	●	●	●		●
	Pursue legal action against AaaS providers and subcontractors.					●
	Encourage technical limits on malware payload jurisdiction.		●	●	●	

A set of policies successful at countering the proliferation of offensive cybersecurity capabilities will need better tools to understand and shape proliferation activities before it is able to impose new costs or limit activity. In the case of AaaS firms, we propose new policies to expand currently available counterproliferation tools and make them more directly effective against AaaS firms. Because these firms span a variety of clientele and operate in different jurisdictions, a coalition approach will be needed. An effective strategy to counter the proliferation of offensive cybersecurity capabilities should be built on a foundation of **international partnership** and strive to **understand, shape,** and, in time, **limit** these firms, thereby better countering a substantial channel for the proliferation of offensive cyber capabilities.

1. UNDERSTAND & PARTNER

The market in which AaaS firms participate is not bound to a single geographical jurisdiction. Instead, these firms transact in markets around the world. The three case studies laid out in this report are by no means the only companies actively developing offensive cyber capabilities—an entire ecosystem of private organizations exist that actively sell from one or more pillars of offensive cyber capability development. Policy makers must better understand this reality and build a strategy to counter the proliferation of offensive cybersecurity capability on a firm foundation of international partnership. While some private organizations sell to the US government and its allies, some of these same organizations may be

concurrently selling capabilities to parties that specifically target these same states. The defense that a company is selling only to “Western clients” or “NATO states” does little to rebut this notion. A better understanding of these vendors is necessary to ensure that the United States and its allies are not unknowingly funding additional forms of cyber-proliferation they may deem unacceptable.

Recommendation 1.1:

Build a coalition of like-minded partners.



The realities of the AaaS ecosystem are such that no single state or government can meaningfully reshape the market on its own. However, a coalition of like-minded states, acting in coordination with one another, can have an appreciable impact on the sellers in the market—the AaaS firms themselves—and could represent a substantial portion of the buyers in the market.

NATO and its strategic partners, or the Organization for Security and Co-operation in Europe (OSCE) and its partners for cooperation, both represent a solid foundation on which a coalition could be built. The United States and its traditional allies—especially those within whose jurisdiction AaaS firms are incorporated, such as Israel, France, Italy, and the United Kingdom—should seek to leverage these existing partnerships to align efforts to intervene in AaaS markets and counter the proliferation of OCC. Notably, certain adversary states, including Russia and China, may hold common interest in countering the proliferation of AaaS and OCC and may be willing partners. Similarly, Lin and Trachtman’s recommendations for cyber export control revision suggest that any coalition should include “countries that might not otherwise be permitted destinations ... for maximum effectiveness.”¹²⁶

Recommendation 1.2:

Elevate the issue of offensive cybersecurity capabilities proliferation in international forums.



Today, cyber foreign policy time, energy, and resources are predominantly focused on the development of norms and law, law enforcement cooperation, and cybersecurity capacity building. These are important efforts to maintain the stability of the international system given the increasing importance of cybersecurity in relations between nations. However, these efforts do little to prevent the spread of OCC. Elevating the issue of countering the proliferation of OCC in international forums will afford governments another tool to both coordinate action and shame bad actors in the space.

The United States and a coalition of like-minded partners should seek to elevate the issue of OCC proliferation in relevant international forums by surfacing the issue as an area for study and international cooperation in relevant working groups and organizations, including the United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security and the Open-ended Working Group, the OSCE, and NATO.

Recommendation 1.3:

Pass “Know Your Vendor” laws or regulations.



To help policy makers better understand the AaaS ecosystem, coalition members should pass or create “Know Your Vendor” (KYV) laws or regulations within their technology acquisition processes. These laws and regulations would provide government clients with the ability to check where their prospective supply chain might include firms on restricted entity lists before awarding contracts. Implementing KYV laws in coalition states would provide more transparency with regards to unsavory contractor-subcontractor relationships and help limit AaaS transactions with more opaque vendors or those knowingly transacting with parties under sanction. KYV laws would also provide more detailed information in freedom of information requests to governments receiving these services, a boon to researchers, civil society, and oversight within government. These KYV laws would apply to, for example, FBI acquisitions of iPhone hacking tools,¹²⁷ as well as other US government contracts with wider AaaS organizations, focusing on contracts and transactions between firms and clients, rather than the products that they sell.

To create a KYV law or regulation in the United States, the US Federal Acquisition Regulatory Council should issue a proposed update to the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) mandating that any company bidding for a government contract for cyber operations, or selling offensive cyber capabilities to the government, must disclose a list of their vendors and customers, as well of those of any parent corporate or holding entity, to the contracting agency as part of the bid.

¹²⁶ Lin and Trachtman, “Using International Export Controls to Bolster Cyber Defenses.”

¹²⁷ Ellen Nakashima, “Comey Defends FBI’s Purchase of iPhone Hacking Tool,” *Washington Post*, May 11, 2016, https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html.

2. SHAPE

To provide additional incentives for private organizations developing offensive cyber capabilities to proliferate responsibly, the United States and its allies, especially the EU and its member states, should also work to shape the AaaS market. For the United States, the first step is acknowledging that a market for these capabilities exists and valuing vendors accordingly. Shaping the market involves restricting and influencing the behavior of both buyers and sellers in the market. This focuses on actors that specifically provide or purchase services to conduct offensive cyber operations, rather than companies selling legitimate technical software often misused for those purposes.

Recommendation 2.1:
Develop ban lists for vendors that are caught selling capabilities to states or entities on published lists of concern.



A crucial tool for shaping AaaS firms is tying their penalties to their customers and linking responses to violations of rules or regulations concerning the sale of offensive cyber capabilities to the range of incentives shaped by statecraft. Most governments keep lists of states and entities of concern. In the United States, these lists include the Entity List,¹²⁸ the Denied Persons List,¹²⁹ and the Foreign Terrorist Organization designation,¹³⁰ among others. Coalition states should block companies that are caught misusing cyber capabilities or selling capabilities to states or entities on lists of concern from consideration in future government contracts, and further penalize their customers and partners. This latter penalty could include limits on foreign military sales transactions or

foreign aid and equivalent measures by EU member states. States have a reasonable interest in using both carrots and sticks to shape their national security outcomes and this would only elevate OCC proliferation as a consideration. This would help tie counter-proliferation of offensive cyber capabilities to broader foreign policy and national security agendas, especially in tense bilateral relationships.¹³¹

Recommendation 2.2:
Standardize risk assessment for the AaaS industry.



Some, perhaps most, AaaS companies will likely begin their own risk assessment procedures to ensure they do not partner with banned organizations and customers or those that might cause them to be penalized. To help companies self-regulate, standardizing risk assessment procedures to evaluate which potential customers might become future liabilities would help assist companies with adoption of KYV laws. Standardized risk assessment templates could be developed in partnership with relevant civil society organizations, and would empower companies to make responsible decisions around proliferation. Failure to produce this kind of due diligence on challenge by the company's home government or another relevant government could be grounds for penalty or submitted as evidence of willing disregard in pursuit of a ban. Alternatively, regular government audits of risk assessment procedures would routinize compliance, identifying problematic practices at an early stage.

In this way, governments could act as a trusted intermediary between civil society organizations recommending standards and rigorous risk assessment processes on the one hand, and AaaS firms on the other. In general, extending

¹²⁸ "Entity List," US Department of State, accessed January 24, 2021, <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>.

¹²⁹ "Denied Persons List," US Department of State, accessed January 24, 2021, <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list>.

¹³⁰ "Foreign Terrorist Organizations," US Department of State, accessed January 24, 2021, <https://www.state.gov/foreign-terrorist-organizations/>.

¹³¹ Others go further, recommending the inverse of this approach: rather than banning certain vendors or focusing on states of concern, instead creating a broad "validated user regime" that is positively, rather than negatively, policed. See Lin and Trachtman, "Using International Export Controls to Bolster Cyber Defenses."

a positive obligation to AaaS vendors to understand the conduct of their customers is critical to overcoming claims of ignorance, however willful. This could complement educational services from state regulatory authorities, like the US Department of Commerce’s Bureau of Industry and Security, which already provides guidance on existing foreign sales and export control.¹³²

**Recommendation 2.3:
Incentivize corporate ethics committees.**



In addition to incentivizing firms to conduct standardized risk assessments, the US government and its partners and allies should use government procurement and contracts to incentivize AaaS firms to create and retain corporate ethics committees. The US government and partner and coalition governments should demand that any AaaS firm they contract with or procure tools or services from already has and maintains a corporate ethics committee that publishes semi-annual public ethics reports on the firm as a condition of eligibility for government contracts. The United States and its allies should also require AaaS firms share with any government customer information about the firm’s risk management program, as well as adequate evidence of this program’s application to recent transactions for a government to make an independent determination of the program’s efficacy and sufficiency. The constitution and processes of an ethics committee and risk management program will of course be determined by the firm itself; however, governments and civil society organizations can contribute recommendations and best practices, as well as assess and comment on any reports produced.

By way of example, NSO Group already claims to have “an ethics committee made up of employees and external counsel [which] vets potential customers based on human rights rankings set by the World Bank and other global bodies.”¹³³ However, the workings of this ethics committee are not publicly available.¹³⁴ Nonetheless, these bodies can have an effect, as former Homeland Security Secretary Jeh Johnson noted in a legal opinion for a subsidiary company of NSO Group, writing that the firm’s “proposed new Human Rights Policy and attendant governance documents of the Group are substantially aligned” with the United Nations Guiding Principles on Business and Human Rights.¹³⁵

**Recommendation 2.4:
Limit foreign military sales and other foreign assistance to states that purchase from banned AaaS providers or use AaaS tools to infringe on human rights.**



Where recommendations 2.1–3, seek to shape the behavior of the sellers in the AaaS market, the US government, together with the coalition recommended in recommendation 1.1, can influence the demand side of the market as well by punishing states that purchase from banned (recommendation 2.1) AaaS providers or use AaaS tools or services to infringe on human rights. To punish bad customers of these firms, the United States and its partners and allies should limit foreign military sales and other foreign assistance to states that purchase AaaS tools or services from banned providers or use AaaS tools to infringe on human rights. This would significantly increase the influence of notional ban lists and help properly tie broader national security interests to this proliferation.

132 “Export Administration,” US Bureau of Industry and Security, accessed January 24, 2021, <https://www.bis.doc.gov/index.php/about-bis/organization/program-offices>.

133 Nicole Perloth, “How Spy Tech Firms Let Governments See Everything on a Smartphone,” *New York Times*, September 2, 2016, <https://perma.cc/3STM-RR9U>; NSO Group expand on this statement elsewhere, see: Josh Rogin, “Washington Must Wake up to the Abuse of Software That Kills,” *Washington Post*, December 12, 2018, <https://perma.cc/L5F2-J2J2>. “The Business Ethics framework is a rigorous internal compliance process designed to ensure that the end-user customers have valid law enforcement or investigative missions, uphold the rule of law, and agree to deploy the technology only for collecting digital evidence in a limited number of critical criminal or national security investigations,” Citizen Lab have juxtaposed this claim with poor World Bank governance indicators in the case of Mexico.

134 Stephanie Kirchgaessner, “Ex-Obama Official Exits Israeli Spyware Firm Amid Press Freedom Row,” *the Guardian*, February 4, 2020, <https://www.theguardian.com/world/2020/feb/04/ex-obama-official-juliette-kayyem-quits-israeli-spyware-firm-amid-press-freedom-row>.

135 Aaron Schaffer, “Israeli Spyware Company Accused of Hacking Activists Hires Lobby Firm,” *AI-Monitor*, January 11, 2020, <https://perma.cc/8HRH-DPDK>.

3. LIMIT

The final pillar of a strategy to counter the proliferation of offensive cyber capabilities should focus on limiting the spread of relevant tools, components, and talent to firms and states that may leverage them against the United States and partners, or in pursuit of human rights violations.

Recommendation 3.1:
Widen the scope of selective defensive vulnerability disclosure.



The United States and coalition governments can limit the breadth and effectiveness of AaaS by conducting defensive disclosure of vulnerabilities known to be leveraged by banned AaaS firms or in tools violating standards of risk management and behavior. This can range from accelerating Vulnerabilities Equities Process (VEP) decisions, especially if a subject software vulnerability is observed in AaaS operations, to scaling the capabilities of the US Cybersecurity and Infrastructure Security Agency (CISA), law enforcement, and other government organizations to expose and help mitigate actor tactics, tools, and procedures for these operations.

Given the precedent of the NSA and FBI's joint publication of Russian hacking tools in August of 2020,¹³⁶ creating processes to encourage additional joint disclosures to selectively burn capabilities from firms that are direct proxies or contractors of adversaries would also be beneficial. The EU can follow member state actions coordinated with the United States or following a similar model. Disclosing capabilities in commercial sale predicated on some measure of secrecy does pose legal challenges, but none which would stand up to the range of legitimate national security interests under which this kind of action should take place. While this kind of selective disclosure may only temporarily

impede AaaS firms working outside of accepted customer relationships, it does create unanticipated costs to retool and, if done successively, could reshape the economics of AaaS for some firms.

Recommendation 3.2:
Establish post-employment restrictions for former government cybersecurity employees.



While focusing on AaaS and other OCC vendor organizations will shape organizational behavior, one of the larger cross-cutting issues across all OCC vendors is the movement of their employees and associated knowledge, especially post-employment. As seen in the above case studies, many of AaaS firms go out of their way to recruit former government employees from the cyber, signals intelligence (SIGINT), or intelligence communities.

This is a particular challenge for the United States, which should require any former government employees or contractors holding a security clearance and subject to a specific list of sensitive job functions/titles/roles to notify the office of the director of national intelligence (DNI) and their home agency of any change in employment for up to ten years after leaving a defined sensitive role. This would provide a modicum of information about the movement of these individuals and their associated professional expertise and skills, providing US intelligence and the defense community greater opportunity to limit exposure of this knowledge to unsuitable states and non-state groups through existing legal means (a similar problem to that faced elsewhere in the US intelligence community).¹³⁷ This risk is highlighted by the DarkMatter case, but also in the portability of ENFER staff's expertise in exploitation and offensive research. This movement of still relatively rare talent represents an obvious proliferation risk.

¹³⁶ Christopher Bing, "NSA, FBI Expose Russian Intelligence Hacking Tool: Report," Reuters, August 13, 2020, <https://www.reuters.com/article/us-usa-cyber-russia-idUSKCN2592HY>.

¹³⁷ Philip Caruso, "How to Take Care of an Ex-Spy," Foreign Policy, June 14, 2019, <https://foreignpolicy.com/2019/06/14/how-to-take-care-of-an-ex-spy/>.

Recommendation 3.3: Pursue legal action against AaaS providers and subcontractors.



For AaaS providers and sub-contractors clearly connected to developing offensive cyber capabilities of adversary governments, indictments and court cases may prove to be an effective tool. Continuing and expanding existing legal action against AaaS providers could impose financial and business costs on an organization, name and shame individuals engaged in such business, or shut down operations entirely through arrests or takedowns. This recommendation focuses solely on criminal cases, given that governments have limited scope in civil litigation other than becoming an attractive jurisdiction for civil lawsuits against spyware vendors.

Legal action should include encouraging the DOJ to unseal classified indictments on AaaS providers and subcontractors, whenever possible, to assist in public naming and shaming of these actors. Creating additional avenues of collaboration between the FBI, Interpol, and other European law enforcement agencies to collaborate in investigations against AaaS firms would also encourage international efforts to subdue known actors engaged in developing offensive cyber capabilities of adversary governments, or corporate espionage against US and other firms. The latter would build upon previous DOJ corporate espionage-related indictments against both private firms¹³⁸ and individuals,¹³⁹ ideally triggering additional probes in other countries.¹⁴⁰

Recommendation 3.4: Encourage technical limits on malware payload jurisdiction.



The US government should also drive offensive security vendors to limit the scope of their products through internal technical limitations, such as geofencing products and services and imposing penalties for clients that deviate from specified contract behavior. Such limitations would prevent additional proliferation and/or misuse of vendor products by customers who may reuse an offensive product against targets in the United States or EU member states—thus risking penalties for the original vendor. These limitations could also prevent misuse of vendor products by customers who may reuse an offensive product against vulnerable populations—providing a technical basis to support narrow contractual limits on use. Limiting the behavior of OCC products would also help constrain proliferation through unwitting spread of malware.¹⁴¹

Technical limitations could include behaviors such as ensuring that the malware will only run for a certain period after the time of sale, and only within certain countries. NSO Group suggests their software “is only licensed to operate in countries approved under our Business Ethics Framework and the product will not operate outside of approved countries.”¹⁴² This includes the United States; the company claims that “NSO software is specifically designed to not function on US phone numbers and cannot be used on phones with US area codes.”¹⁴³ Technical limits are not a panacea and they would involve substantial buy-in from AaaS vendors, but they would provide more mechanistic means of regulation to compliment other reforms like KYV laws and contracting penalties.

138 “Private Investigators Indicted in E-Mail Hacking Scheme,” The United States Attorney’s Office, Northern District of California, February 11, 2015, <https://www.justice.gov/usao-ndca/pr/private-investigators-indicted-e-mail-hacking-scheme>.

139 “Seven International Cyber Defendants, Including ‘APT41’ Actors, Charged in Connection with Computer Intrusion Campaigns Against more than 100 Victims Globally,” US Department of Justice, September 16, 2020, <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>.

140 William Turton, “U.S. Investigating Hacker Ring Paid to Target Corporate Critics,” *Bloomberg*, June 10, 2020, <https://www.bloombergquint.com/technology/u-s-investigating-hacker-ring-paid-to-target-corporate-critics>.

141 “NSO Group v. WhatsApp,” US Court of Appeals for the Ninth Circuit, December 12, 2020, <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v.-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf>.

142 Marczak et al., “Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries.”

143 The Mexico case of a US phone number was targeted but not infection, see: Stephanie Kirchgaessner and Jon Swaine, “US Senator to Investigate If Foreign Spyware Used to Target Americans,” *the Guardian*, November 26, 2019, <https://perma.cc/6Z9H-CJ5Z>; and O’Neill “Inside NSO, Israel’s Billion-Dollar Spyware Giant.”

Conclusion

Controlling proliferation of offensive cyber capabilities through AaaS firms, which speed and scale up the ability of foreign governments to conduct offensive cyber operations, is an important task. For the United States, as an example, this task becomes even more urgent as some AaaS firms exploit major US technology firms and target US citizens, or recruit US cybersecurity practitioners to do so. States will pursue offensive capabilities in cyberspace, and, as in other domains of national security acquisitions, private sector firms play an increasingly important role in the development and diffusion of those capabilities. This is particularly true for smaller states or those with more nascent offensive cyber programs. The expansion of this private industry, unchecked by granular state controls and strategy to effectively balance national security objectives in limiting the proliferation of OCC, risks accelerating harm to both the public and state's own security interests.

The framework of analysis presented in this work identifies potential mechanisms of proliferation and the equities harmed by the unconstrained interactions within AaaS markets. This framing further highlights the unique character of this problem—activities previously restricted to clandestine intelligence liaison relationships, or opaque military-to-military partnerships, have now become matters profitably pursued by private firms largely independent of traditional concepts of state control exercised over offensive capabilities in kinetic conflict. In turn, this expands the conversation over policy responses intended to mitigate the consequences and costs from the negative outcomes of such proliferation. It is unlikely that states will agree to entirely forego the utility of privately developed expertise and offensive capabilities in advancing operational objectives and programmatic maturity, particularly in cases where specific national interests may dictate involvement at greater than arm's length. However, states may

be incentivized to conduct future engagements with greater restraint, increased oversight, and in ways that are mindful of the negative externalities and failures modes encountered in past cases. It will remain in the international community's interest to see such incentives develop and find, at least, tacit acceptance in practice, even if formal normative agreement remains unlikely in the near term.

This report identified a number of tradeoffs in managing the flow of these OCC through AaaS markets, emphasizing the need to both **understand & partner** and **shape** these transactions. **Limiting** this proliferation entails choices about relative national priorities which we do not address here, but which should be a priority for future work. For the EU in particular, if European states do not grasp the varied risks of OCC proliferation, especially in the form of AaaS companies, this risks undermining not only their image as a competent and principled regulatory power with global reach but could also fracture a fragile consensus over security policy between key European states, especially France and Germany. The recommendations of this report are designed to help European states shape an effective and transparent AaaS market in line with the EU's stated values. How and where to transition from shaping to overt limitation is deserving of further scrutiny.

In the broad context of constraining malicious cyber behavior, interventions to counter the proliferation of OCC have been limited in scope. This report and its counterpart, "A Primer on the Proliferation of Offensive Cyber Capabilities," provide a more granular mapping of the proliferation of OCC by focusing on AaaS firms and their marketplace. In sharing policy recommendations as a means to grant states better tools to understand, shape, and limit this proliferation, this report seeks to underline the shortcomings of existing policy as much as the requisite urgency of reform.

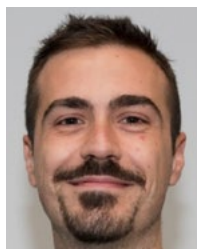
About the Authors



Winnona DeSombre is a nonresident fellow with the Atlantic Council's Cyber Statecraft Initiative. She works as a security engineer at Google's Threat Analysis Group, tracking targeted threats against Google users. In recent years, Winnona co-authored the Harvard Belfer Center's National

Cyber Power Index, constructed risk rule calculation software to combat social media influence campaigns, spoke at the Forbes 30 under 30 Summit and presented original research at DEFCON.

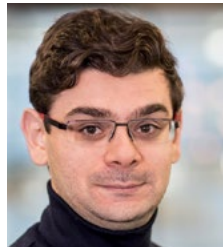
Her research has also been featured in publications including Foreign Policy, VICE's Motherboard, and CyberScoop. Winnona is a vocal advocate for women in cyber security: when not ruminating on cyber policy, she spends her time volunteering for Women in Security and Privacy, and has taught courses on cyber security, ethical hacking and personal security through the nonprofit GirlSecurity.



Michele Campobasso is a PhD candidate at the Security Group of Eindhoven University of Technology under the supervision of Dr. Luca Allodi. He has completed his studies cum laude in Computer Sciences and Engineering at Alma Mater Studiorum - University of Bologna, Italy in 2019; the thesis is entitled

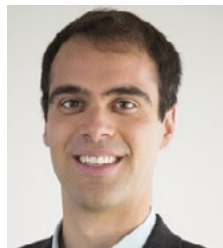
"CARONTE: a Crawler for Adversarial Resources Over Non Trusted, high-profile Environments" and has been published in the proceedings of the 1st Workshop on Attackers and Cyber-Crime Operations (WACCO) held at IEEE European Symposium on Security and Privacy 2019 in Stockholm, Sweden.

His research interests aim at characterizing threats emerging from underground black markets, how they're framed in the threat scenario and studying the foundational problems of threat intelligence obtained from underground surveillance.



Dr. Luca Allodi is an assistant professor in the Security Group of the Eindhoven University of Technology (TU/e). His research focuses on vulnerability laws, with a strong accent on attackers' behavior and strategies, seeking quantitative answers to the economics of vulnerability exploitation and the

management of cyber risk. His research looks for technical, economic, and strategic factors that drive vulnerability exploitation 'in the wild'. To this aim, he investigates the dynamic optimization problems the attacker solves when engineering a new attack, the underground markets in which the attackers operate, the technology they employ, and the rates at which attacks are delivered to the final users. This research draws from several fields, including computer security, economics, risk analysis, and criminology. Luca is currently working on new ways to integrate security metrics with cyber attacks economics; in particular, he is interested in understanding if analysis of new trends in cybercrime attacks (APTs, black markets, botnet rentals...) can be exploited to improve current metrics for security.



Dr. James Shires is an assistant professor at the Institute for Security and Global Affairs, University of Leiden and is a non-resident fellow with the Atlantic Council's Cyber Statecraft Initiative. He holds a DPhil in International Relations from the University of Oxford, an MSc from Birkbeck College, University of London and a BA from the

University of Cambridge. His research examines cybersecurity in the Middle East, focusing on the interaction between threats to individuals, states and organizations, new regional dynamics, and the development of cybersecurity expertise.



JD Work is a nonresident senior fellow with the Atlantic Council's Cyber Statecraft Initiative. He serves as the Bren Chair for Cyber Conflict and Security at the Marine Corps University, where he leads research to develop the theory, practice, and operational art of the cyber warfighting function, and to explore the wider role of the cyber instrument in national security strategy, and the future defense competition and stability problem space.

Mr. Work has over two decades experience working in cyber intelligence and operations roles for the private sector and US government. He previously directed multiple international research programs to provide insight into the emerging strategic issues, economic consequences, and technology implications created by hostilities in the virtual domain. This work has sought to establish a reliable baseline of observations regarding the engagements, follow on effects, capabilities, doctrine, and drivers behind the antagonistic action of potential combatants in the networked environment, in order to support early warning, crisis management and crisis prevention in and through cyberspace.

Mr. Work holds additional affiliations with Columbia University's School of International and Public Affairs, Saltzman Institute of War and Peace Studies as well as George Washington University, Elliot School of International Affairs. He further serves as a senior advisor to the US Cyberspace Solarium Commission.



Robert Morgus is a senior director for the US Cyberspace Solarium Commission, where he directs research and analysis for Task Force Two. At the Commission, Morgus has led the development of the ecosystem pillar of the Commission's final report as well as the Pandemic White Paper and the Supply Chain White Paper.

Previously, he helped build New America's Cybersecurity Initiative, where he headed the organization's international cyber policy work. While at New America, his research focused on mechanisms to counter the spread of offensive cyber

capability, cybersecurity and international governance, and Russian internet doctrine. In the past, he has authored reports on international cybersecurity norms, internet governance, cybersecurity insurance, amongst others.

Morgus has spoken about cybersecurity at a number of international forums including NATO's CyCon, the Global Conference on Cyberspace at The Hague, and Cy Fy 2015 in New Delhi, India. His research has been published and recognized by the New York Times, Slate, the IEEE, peer-reviewed academic journals, and numerous other national and international media outlets. Morgus serves as a member of the Research Advisory Network for the Global Commission on Internet Governance, as well as the Global Forum on Cyber Expertise, and has served as an expert advisor for the World Economic Forum.



Patrick Howell O'Neill is the cybersecurity senior editor for MIT Technology Review. He covers national security, election security and integrity, geopolitics, and personal security: How is cyber changing the world? Before joining the publication, he worked at the Aspen Institute and CyberScoop covering cybersecurity from Silicon Valley and Washington DC.



Dr. Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on the role of the technology industry in geopolitics, cyber conflict, the security of the internet, cyber safety, and growing a more capable cybersecurity policy workforce. Previously, he was a Senior

Security Strategist with Microsoft handling cloud computing and supply chain security 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.

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

*Richard W. Edelman

*C. Boyden Gray

*Alexander V. Mirtchev

*John J. Studzinski

TREASURER

*George Lund

DIRECTORS

Stéphane Abrial

Todd Achilles

*Peter Ackerman

Timothy D. Adams

*Michael Andersson

David D. Aufhauser

Colleen Bell

*Rafic A. Bizri

*Linden P. Blue

Philip M. Breedlove

Myron Brilliant

*Esther Brimmer

R. Nicholas Burns

*Richard R. Burt

Michael Calvey

Teresa Carlson

James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

*George Chopivsky

Wesley K. Clark

*Helima Croft

Ralph D. Crosby, Jr.

*Ankit N. Desai

Dario Deste

*Paula J. Dobriansky

Joseph F. Dunford, Jr.

Thomas J. Egan, Jr.

Stuart E. Eizenstat

Thomas R. Eldridge

*Alan H. Fleischmann

Jendayi E. Frazer

Courtney Geduldig

Thomas H. Glocer

John B. Goodman

*Sherri W. Goodman

Murathan Günal

Amir A. Handjani

Katie Harbath

Frank Haun

Michael V. Hayden

Amos Hochstein

*Karl V. Hopkins

Andrew Hove

Mary L. Howell

Ian Ihnatowycz

Wolfgang F. Ischinger

Deborah Lee James

Joia M. Johnson

*Maria Pica Karp

Andre Kelleners

Astri Kimball Van Dyke

Henry A. Kissinger

*C. Jeffrey Knittel

Franklin D. Kramer

Laura Lane

Jan M. Lodal

Douglas Lute

Jane Holl Lute

William J. Lynn

Mark Machin

Mian M. Mansha

Marco Margheri

Chris Marlin

William Marron

Neil Masterson

Gerardo Mato

Timothy McBride

Erin McGrain

John M. McHugh

H.R. McMaster

Eric D.K. Melby

*Judith A. Miller

Dariusz Mioduski

*Michael J. Morell

*Richard Morningstar

Dambisa F. Moyo

Virginia A. Mulberger

Mary Claire Murphy

Edward J. Newberry

Thomas R. Nides

Franco Nuschese

Joseph S. Nye

Ahmet M. Ören

Sally A. Painter

Ana I. Palacio

*Kostas Pantazopoulos

Alan Pellegrini

David H. Petraeus

W. DeVier Pierson

Lisa Pollina

Daniel B. Poneman

*Dina H. Powell McCormick

Robert Rangel

Thomas J. Ridge

Lawrence Di Rita

Michael J. Rogers

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

Rajiv Shah

Wendy Sherman

Kris Singh

Walter Slocombe

Christopher Smith

James G. Stavridis

Michael S. Steele

Richard J.A. Steele

Mary Streett

*Frances M. Townsend

Clyde C. Tuggle

Melanne Verveer

Charles F. Wald

Michael F. Walsh

Gine Wang-Reese

Ronald Weiser

Olin Wethington

Maciej Witucki

Neal S. Wolin

*Jenny Wood

Guang Yang

Mary C. Yates

Dov S. Zakheim

HONORARY DIRECTORS

James A. Baker, III

Ashton B. Carter

Robert M. Gates

James N. Mattis

Michael G. Mullen

Leon E. Panetta

William J. Perry

Colin L. Powell

Condoleezza Rice

Horst Teltschik

John W. Warner

William H. Webster

**Executive Committee Members*

List as of February 8, 2021



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.

© 2021 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

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

(202) 463-7226, www.AtlanticCouncil.org