Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

#ACcyber

ISSUE BRIEF

A Primer on the Proliferation of Offensive Cyber Capabilities

MARCH 2021

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

EXECUTIVE SUMMARY

Offensive cyber capabilities run the gamut from sophisticated, long-term disruptions of physical infrastructure to malware used to target human rights journalists. As these capabilities continue to proliferate with increasing complexity and to new types of actors, the imperative to slow and counter their spread only strengthens. But to confront this growing menace, practitioners and policy makers must understand the processes and incentives behind it. The issue of cyber capability proliferation has often been presented as attempted export controls on intrusion software, creating a singular emphasis on malware components. This primer reframes the narrative of cyber capability proliferation to be more in line with the life cycle of cyber operations as a whole, presenting five pillars of offensive cyber capability: *vulnerability research and exploit development, malware payload generation, technical command and control, operational management, and training and support*. The primer describes how governments, criminal groups, industry, and Access-as-a-Service (AaaS) providers work within either self-regulated or semi-regulated markets to proliferate offensive cyber capabilities and suggests that the five pillars give policy makers a more granular framework within which to craft technically feasible counterproliferation policies without harming valuable elements of the cybersecurity industry. These recommended policies are developed in more detail, alongside three case studies of AaaS firms, in our companion report, *Countering Cyber Proliferation: Zeroing in on Access as a Service.*

INTRODUCTION

The proliferation of offensive cyber capabilities (OCC) has often been compared with nuclear proliferation and stockpiling. Nuclear and cyber are two very different threats, especially in their regulatory maturities, but in both of them a multitude of bilateral and multilateral treaties have been created and then sidestepped, acceded to, expanded, and abandoned like steps in a dance. Regulatory and policy aspects in the OCC domain are particularly difficult due to the elusive nature of cyber capabilities, and the difficulty of measuring them, especially in the absence of a clear framework that defines and maps them to the broader picture of international equilibria. Offensive cyber capabilities are not currently cataclysmic, but are instead quietly and persistently pernicious. The barrier to entry in this domain is much more of a gradual rise than a steep cliff, and this slope is expected to only flatten increasingly over time.[1] As states and non-state actors gain access to more and better offensive cyber capabilities, and the in-domain incentives to use them,[2] the instability of cyberspace grows. Furthermore, kinetic effects resulting from the employment of offensive cyber capabilities, the difficulties in the attribution process of attacks caused by an invisible militia, and the lack of mature counterproliferation regimes bring the problem to a geopolitical scale.

Creating a counterproliferation regime in cyberspace has confounded policy makers for over a decade. As the number of state-sponsored cyber actors continues to rise alongside the severity of cyber attacks, the issue has become even more pressing.

The renewed vigor with which the European Union (EU) has seized upon this topic and the arrival of new occupants in the locus of political authority in the United States present an opportunity to provide the debate with a more complete context and to more precisely frame the interests of the players involved. This effort sits within the body of work that frames the construction, sale, and use of OCC as a question of proliferation.[3] Policy efforts should seek to reduce the utility of these capabilities and influence the incentives of the parties involved in the process of proliferation, rather than seeking vainly to block proliferation entirely.[4]

[1] Adam Segal, "The Code Not Taken: China, the United States, and the Future of Cyber Espionage," *Bulletin of the Atomic Scientists* 69, no. 5 (November 27, 2015), https://www.tandfonline.com/doi/abs/10.1177/0096340213501344.

[2] Michael P. Fischerkeller and Richard J. Harknett, "Cyber Persistence, Intelligence Contests, and Strategic Competition," In *Policy Roundtable: Cyber Conflict as an Intelligence Contest*, eds. Robert Chesney and Max Smeets, (Texas National Security Review, September 17, 2020), https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.

[3] Trey Herr, "Malware Counter-Proliferation and the Wassenaar Arrangement," *Proceedings of the 8th International Conference on Cyber Conflict*, 2016, https://dx.doi.org/10.2139/ssrn.2711070.

[4] Trey Herr, "Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle," *The Cyber Security Project*, Harvard Kennedy School, Belfer Center for Science and International Affairs, June 2017, https://digital.hbs.edu/wp-content/uploads/2017/09/CounteringProliferationofMalware.pdf; Robert Morgus, Max Smeets, and Trey Herr, "Countering the Proliferation of Offensive Cyber Techniques," GCSC Briefings from the Research Advisory Group, 2017, http://maxsmeets.com/wp-content/uploads/2018/09/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017-161-187.pdf, 161-187.

OFFENSIVE CYBER CAPABILITIES: SEEING THE WHOLE CHAIN

The failure of OCC counterproliferation stems from a poor understanding of how cyber capabilities are created and spread. The majority of contemporary policy efforts, including the Wassenaar Arrangement, are meager transplants of Cold War–era nonproliferation strategies into cyberspace. These efforts, while part of an existing toolkit to counter proliferation efforts, frame OCC as tools and work to block their sale through export control rules; there are myriad critiques of this approach.[5] The Wassenaar Arrangement accounted for some of this, controlling not the malware itself (which it has dubbed "intrusion software") but software that was designed for command-and-control finalities.

However, offensive cyber capabilities consist of more than just malware and its command and control. Stuxnet was malware attributed to Israel and the United States,[6] a worm that did not rely on command-and-control networks.[7] The malware was designed to target specialized hardware (SCADA systems) adopted to control machinery and industrial processes, including centrifuges for obtaining nuclear material, and to destroy them by causing controlled malfunctions, ultimately slowing down the Iranian nuclear program.[8] Not only was the malware incredibly tailored to the specific hardware in Iran's Natanz nuclear site, but the malware itself also used five 0day-exploits,[9] was regularly updated by malware developers, and likely required heavy collaboration between Israeli and US intelligence counterparts to deploy. The malware delivery mechanism, testing processes, and deployment of the Stuxnet malware through Operation Olympic Games were the culmination of multiple offensive cyber capabilities much broader than just command and control. To accurately frame OCC, it is therefore crucial to be able to distinguish and separate different offensive capabilities—to understand OCC as a chain of commodities, skills, and activities, moving away from a singular emphasis on malware components and toward the life cycle of a cyber operation.

In this document, we introduce five pillars of offensive cyber capability as a means to characterize the technical and operational foundations of OCC. The five pillars are *vulnerability research and exploit development, malware payload development, technical command and control, operational management, and training and support*. Table 1 provides an overview of these pillars.

The next sections develop a more detailed picture of the markets in which these transactions take place and describe the five pillars of this chain of OCC.

[5] Gozde Berkil, "Cybersecurity and Export Controls," The Fletcher School, Center for Law and International Governance, December 10, 2018, https://sites.tufts.edu/cilg/2018/12/10/cybersecurity-and-export-controls/; Dorothy Denning, "Reflections on Cyberweapons Controls," *Computer Security Journal* 16, no. 4 (2000): 43-53, https://faculty.nps.edu/dedennin/publications/Reflections_on_Cyberweapons_Controls.pdf; "Export Controls," Electronic Frontier Foundation, accessed January 19, 2021, https://www.eff.org/issues/export-controls; Sergey Bratus, DJ 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 College, October 9, 2014, https://www.cs.dartmouth.edu/~sergey/wassenaar/wassenaar-public-comment.pdf; Sergey Bratus, "The Wassenaar Arrangement's Intent Fallacy," Bureau of Industry and Security, US Department of Commerce, December 8, 2015, https://tac.bis.doc.gov/index.php/documents/pdfs/320-wa-intent-fallacy-bratus-comments/file; Thomas Dullien, Vincenzo Iozzo, and Mara Tam, "Surveillance, Software, Security, and Export Controls: Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting," Bureau of Industry and Security, US Department of Commerce, February 10, 2015, https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file; Mailyn Fidler, "Proposed U.S. Export Controls: Implications for Zero-Day Vulnerabilities and Exploits," Lawfare, June 10, 2015, https://www.lawfareblog.com/proposed-us-export-controls-implications-zero-day-vulnerabilities-and-exploits.

[6] David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program, IEEE Spectrum, February 26, 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet; Nate Anderson, "Confirmed: US and Israel Created Stuxnet, Lost Control of It," https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/; "What Is Stuxnet?" McAfee, accessed January 28, 2021, https://www.mcafee.com/enterprise/it-it/security-awareness/ransomware/what-is-stuxnet.html.

[7] Kushner, "The Real Story of Stuxnet."

[8] Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langner Group, November 2013, https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

[9] A zero day (or 0day) is a vulnerability that is currently unknown to the software vendor and the organization whose system the vulnerability affects, and for which a patch does not exist.

TABLE 1. THE FIVE PILLARS OF OFFENSIVE CYBER CAPABILITY PROLIFERATION

	Definition	Government examples	Criminal examples	industry examples	AaaS examples
VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT	Discovered vulnerabilities, or disclosure programs that facilitate the proliferation of discovered vulnerabilities and written exploits	Chinese intelligence community vulnerability research and exploitation, specifically within the MSS and its associated CNNVD	Exploit kits sold on underground forums	Bug bounty programs, vulnerability disclosures, Zerodium	NSO Group's use of a WhatsApp 0day
MALWARE PAYLOAD DEVELOPMENT	Any malware or tool written or used by attackers to conduct offensive cyber operations, or any forum that encourages or conducts exchange of malware	Custom malware developed by state teams that is reverse engineered and published by malware analysts	Commercial malware market	Red-team tools developed and sold through commercial offerings and companies; posting malware for research on GitHub	NSO Group's Pegasus spyware
TECHNICAL COMMAND AND CONTROL	Technologies aimed at supporting offensive cyber operations, e.g., bulletproof hosting, domain name registration, server side command-and-control software, VPN services, or delivery accounts involved with the initial creation of an offensive cyber operation	IPs and domains attributed to state operations by threat intelligence reports	Bulletproof hosting and other pre-bullet command-and-control infrastructure	Test servers built to send phishing tests against one's own companies, infrastructure used for penetration testing services	Infrastructure used by Appin Security for Operation Hangover
OPERATIONAL MANAGEMENT	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	Chain of command within and organization of government intelligence agencies	Criminal outsourcing, ransomware affiliate programs	Delegation of duties within a red-team exercise; escalation policies during an incident	Good Harbor Consulting's organizational management of UAE DREAD cyber capabilities
TRAINING AND SUPPORT	Training or education provided on the offensive cyber operation process, expanding the number of trained professionals and creating connections between them that facilitate the growth of OCC	NSA's National Cryptologic School or other government-sponsored cyber training program	Fraud tutorials, phishing kits, customer support provided within forums	Kali Linux tutorials on YouTube, cyber security certifications, conference trainings and talks	DarkMatter training provided to UAE cyber operators

Note: Abbreviations: MSS: China's Ministry of State Security; CNNVD: China's National Vulnerability Database; AaaS: Access-as-a-Service; VPN: virtual private network; IP: Internet Protocol; OCC: offensive cyber capabilities; UAE: United Arab Emirates; DREAD: the UAE's Development Research Exploitation and Analysis Department; NSA: US National Security Agency.

SEMI- AND SELF-REGULATED MARKETS FOR OCC PROLIFERATION

Providers and developers of OCC can be roughly separated into *self-regulated* and *semi-regulated* spaces. Both spaces provide access to technology such as malware, supporting infrastructures, and vulnerabilities, but differ in their maturities, capacities to innovate, and quality of offerings. Self-regulated spaces operate autonomously, typically through underground internet markets that govern transactions and rules to enforce contracts. Among the most well-known, 0day.today operates in the clearweb and is branded as a marketplace specialized in vulnerability exploits and 0days (albeit of dubious quality), while exploit.in and dark0de operate(d) in the underground as well-regulated forums offering their members a trusted environment to facilitate trade of different products. By contrast, operators in semi-regulated spaces typically act in the open, under the jurisdiction of the state where they operate; among them, the notorious Israeli firm NSO Group states on its website that it provides "authorized governments with technology that helps them combat terror and crime."[10] Both spaces contain actors of varying capabilities, communities, and resources to develop and conduct their own operations. For example, 0day.today provides a loosely regulated environment with little assurance that the exploits therein are effective and undetectable; by contrast, more strongly (self-) regulated markets like exploit.in, operating in the mainly Russian underground space, provide stronger regulation mechanisms aimed at pushing upward the average quality of traded products. Services also vary widely in offered capabilities. These range from supplying individual components to independently developing and conducting whole offensive cyber operations. The accompanying report, *Countering Cyber Proliferation*, provides a breakdown over three case studies of AaaS players of varying capabilities across the proposed five pillars.

Actors present within self- and semi-regulated spaces can further be divided into government, criminal, and private actors enabling Access-as-a-Service (AaaS)—i.e., hack-for-hire actors effectively selling computer network intrusion services to clients. A single cyber operation, depending on the country of origin and nature of attack, can consist of individuals spanning multiple categories (e.g., government and contracting businesses, government and criminal, business and criminal).

In the self-regulated criminal space, heterogeneous underground markets proliferate, ranging from *free* markets that can be easily and freely accessed by any (wannabe) attackers, *pull-in* markets that enable some mechanisms of access regulation via invite from trusted members of the market, to *segregated* marketplaces frequented by highly skilled cybercriminals.[11,12] This progression reflects not only more controlled environments, but also access to more mature and innovative attack capabilities (e.g., in the form of new vulnerabilities, malware, or command-and-control infrastructure).[13]

Similarly, operators in the semi-regulated space also vary in terms of offensive capabilities: from governmental agencies with ample and mature cyber capabilities, able to develop their own attacks and capable of autonomously conducting offensive cyber operations at all levels, to private companies offering legitimate versions of cyber tools with the same capabilities as those that may be misused by criminals. Among these, AaaS organizations also operate in the semi-regulated space, but are different from all other forms of proliferation in that they offer fully fledged offensive services commercially accessible only by accredited actors (e.g., governmental agencies with plentiful resources but little or insufficient internal know-how). These actors offer and develop advanced offensive capabilities to governments due to the prices or funding they are able to receive for providing such services, and their frequent ability to simultaneously conduct research and development, train personnel, and scale businesses.

AaaS groups are known to provide support to governments that need established capabilities, but are incapable of producing them organically. NSO Group is one of the most prominent such vendors, providing services to operations in forty-five countries.[14] The main differences in terms of capabilities that distinguish governments from private actors emerge from the presence of a business model for the latter, which ultimately

[10] "Home," NSO Group, accessed January 28, 2021, https://www.nsogroup.com/; This claim is largely disputed due to the use of their products to conduct attacks against human rights activists and journalists in various countries: 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/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[11] Brian Krebs, "Why Were the Russians So Set against This Hacker Being Extradited?" *Krebs on Security*, November 18, 2019, https://krebsonsecurity.com/2019/11/why-were-the-russians-so-set-against-this-hacker-being-extradited/.

[12] Luca Allodi, M. Corradin, and F. Massacci, "Then and Now: On the Maturity of the Cybercrime Markets, the Lesson that Black-Hat Marketeers Learned," *IEEE Transactions on Emerging Topics in Computing*, 2016.

[13] Ibid.

[14] Marczak et al., "Hide and Seek."

need to remain profitable to operate—a constraint not necessarily as strong for nation states that have developed advanced cyber capabilities. While governments may develop OCC for strategic reasons, AaaS private groups must achieve economic sustainability to continue operations. Nonetheless, Access-as-a-Service firms offer government-level capabilities at private sector speeds.

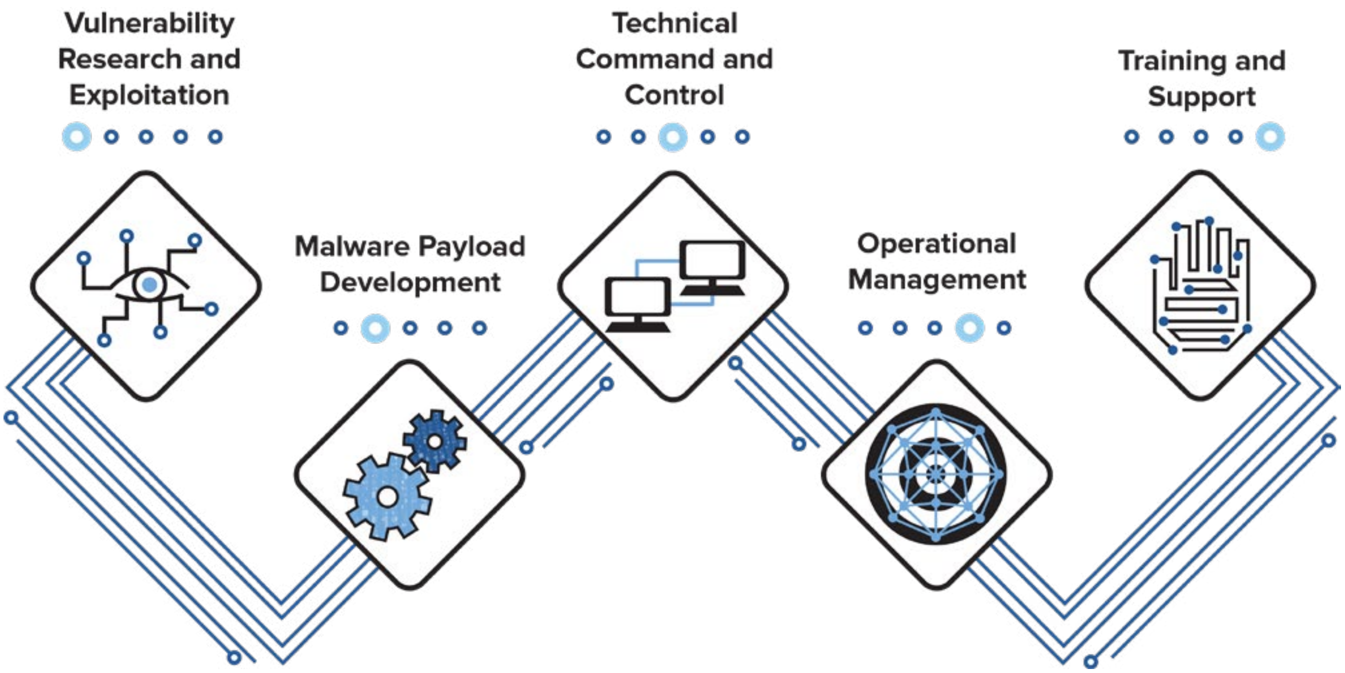
The chain of offensive cyber capabilities encompasses five pillars of activity as laid out below. These pillars are rooted in existing literature and models on cyber operations and capabilities, as well as in public reporting on cyber operations observed “in the wild.” The differences between criminal, government, industry, and AaaS organizations that proliferate these capabilities are explained in the next section. Table 2 provides a bird’s eye view of the landscape across these presented dimensions. Overall, there is a clear progression in offensive capabilities as one moves from the underground markets to private and governmental players; on the other hand, some similarities emerge. In the following pages we provide an in-depth view of the specific capabilities developed across the defined pillars by actors in the self-regulated and semi-regulated spaces from which this overview is derived.

TABLE 2: AVAILABILITY OF TECHNOLOGY FOR EACH PHASE ACROSS MARKETPLACE

	Self-regulated space (Black markets)			Semi-regulated space	
	Free	Pull-in	Segregated	Private - AaaS^^	Government (*)
Vulnerability Research	–	○	◐	●	●
and Exploit Development	–	◐	●	●	●
Malware Payload Development	○	◐	◐	●	●
Technical Command and Control	–	○	◐	◐	●
Operational Management	–	◐	◐	●	●
Training and Support	○	◐	◐	●	●

Notes: Cells indicate the capabilities for a specific pillar for a given actor.
Blank cells with a dash – indicate no capabilities for that specific dimension;
○ indicates the actors have only basic capabilities on that dimension, e.g., obtained by operating automated frameworks;
◐ indicates actors can repurpose and modify existing technologies in that dimension, e.g., to obfuscate known malware/exploit code;
● indicates actors can generate novel methods or efforts in that dimension, e.g., 0day exploits.
(*) Assessment for governments with mature cyber capabilities. ^^AaaS stands for Access-as-a-Service.

THE FIVE PILLARS OF OFFENSIVE CYBER CAPABILITY PROLIFERATION


Vulnerability Research and Exploitation
Malware Payload Development
Technical Command and Control
Operational Management
Training and Support

PILLAR ONE:
Vulnerability Research and Exploit Development

Attackers find vulnerabilities and write exploits to gain a foothold in or access to a target program or device, usually within the context of a multistage operation. This pillar includes research to find the vulnerabilities themselves, as well as disclosure programs and research organizations that facilitate the proliferation of discovered vulnerabilities and written exploits.

A vulnerability is a flaw in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy, usually by catalyzing unexpected behavior.[15] The specific code used to trigger the unexpected behavior by using the vulnerability is called an exploit.[16] An exploit is written for a specific vulnerability and the type of system the vulnerability targets.

Exploiting a vulnerability provides attackers with access to a target system before installing a malware payload that creates the intended final effect. This access becomes especially effective when so-called *zero day vulnerabilities* are involved. A zero day (or 0day) is a vulnerability that is currently unknown to the software vendor and the organization whose system the vulnerability affects, and for which a patch does not exist. Because of this, a well-engineered exploit for that vulnerability will have no defense

[15] "Internet Security Glossary, Version 2," IETF Trust, 2007, https://tools.ietf.org/html/rfc4949.

[16] "Vulnerability," F-Secure, accessed January 19, 2021, https://www.f-secure.com/v-descs/articles/vulnerability.shtml.

until a fix is developed.[17] A number of campaigns attributed to nation states employ zero days:[18] Cyber operations alleged to originate from North Korea,[19] China,[20] Iran,[21] the United Arab Emirates (UAE),[22] South Korea,[23] the United States,[24] and multiple other countries[25] used zero days to increase their access to a target network, download additional malware, or install backdoors onto victim computers.

Because zero days can provide unmatched access when conducting offensive cyber operations, vulnerability research or bug bounty programs are sometimes linked to government organizations to funnel vulnerabilities into state-backed cyber operations. The US Vulnerabilities Equities Process determines whether zero day vulnerabilities are disclosed to the public or withheld for cyber operations on a case-by-case basis.[26] As another example, CNITSEC, an office within China's Ministry of State Security, has operated a Source Code Review Lab out of Beijing since 2003.[27] China's Ministry of State Security has repeatedly been associated with Chinese-backed advanced persistent threats, or APTs, which have conducted cyber operations against US targets.[28]

Vulnerability disclosure can be similarly affected by government organizations conducting offensive cyber operations to prevent patching of targeted systems. China's National Vulnerability Database (CNNVD) is run by CNITSEC. By comparing publication dates of vulnerabilities within the CNNVD and its US counterpart, the National Vulnerability Database (NVD), researchers found that CNNVD beat NVD to publication for 43 percent of all vulnerabilities, except where vulnerabilities were used by Chinese APTs[29] (after that report was released, the CNNVD retroactively altered the publication date of the vulnerabilities in question).[30] Vulnerability research also has legitimate uses for defense within both governments and private companies: By finding vulnerabilities in one's own system prior to exploitation, an organization can update its software, protecting users. Corporate and government-wide bug bounty programs are designed for exactly this purpose, effectively "crowdsourcing" security testing.[31]

States and large criminal groups will also use exploits even after their vulnerabilities have been patched (known as N-days). While generally less effective, these exploits make up a bulk of

[17] A. Ozment, "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting," WEIS, June 2005.

[18] Maddie Stone, "Reversing the Root: Identifying the Exploited Vulnerability in 0-Days Used in-the-Wild," Black Hat USA, August 5, 2020, https://www.blackhat.com/us-20/briefings/schedule/index.html#reversing-the-root-identifying-the-exploited-vulnerability-in--days-used-in-the-wild-20308.

[19] "North Korean Hackers Allegedly Exploit Adobe Flash Player Vulnerability (CVE-2018-4878) against South Korean Targets," *Trend Micro*, February 2, 2018, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/north-korean-hackers-allegedly-exploit-adobe-flash-player-vulnerability-cve-2018-4878-against-south-korean-targets.

[20] Catalin Cimpanu, "Two Trend Micro Zero-Days Exploited in the Wild by Hackers," *ZDNet,* March 17, 2020, https://www.zdnet.com/article/two-trend-micro-zero-days-exploited-in-the-wild-by-hackers/.

[21] Ionut Arghire, "Iranian Hackers Exploit Recent Office 0-Day in Attacks: Report," *Security Week*, May 1, 2017, https://www.securityweek.com/iranian-hackers-exploit-recent-office-0-day-attacks-report.

[22] Kathleen Metrick, Parnian Najafi, and Jared Semrau, "Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill — Intelligence for Vulnerability Management, Part One," *FireEye*, April 6, 2020, https://www.fireeye.com/blog/threat-research/2020/04/zero-day-exploitation-demonstrates-access-to-money-not-skill.html.

[23] Eduard Kovacs, "South Korea–Linked Hackers Targeted Chinese Government via VPN Zero-Day," *Security Week*, April 6, 2020, https://www.securityweek.com/south-korea-linked-hackers-targeted-chinese-government-vpn-zero-day.

[24] Nicole Perloth and Scott Shane, "In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc," *New York Times*, May 25, 2019, https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html.

[25] Metrick et al., "Zero-Day Exploitation Increasingly Demonstrates Access to Money."

[26] White House, "Vulnerabilities Equities Policy and Process for the United States Government," US Government, November 15, 2017, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[27] "China Information Technology Security Certification Center Source Code Review Lab Opened," *Microsoft News*, September 26, 2003, https://news.microsoft.com/2003/09/26/china-information-technology-security-certification-center-source-code-review-lab-opened/.

[28] "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," US Department of Justice, Office of Public Affairs, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[29] Priscilla Moriuchi and Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," *Recorded Future*, November 16, 2017, https://www.recordedfuture.com/chinese-mss-vulnerability-influence/.

[30] Priscilla Moriuchi and Bill Ladd, "China Altered Public Vulnerability Data to Conceal MSS Influence," *Recorded Future*, March 9, 2018, https://www.recordedfuture.com/chinese-vulnerability-data-altered/.

[31] Dale Gardner, "Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing," Gartner Research, June 4, 2018, https://www.gartner.com/en/documents/3877467.

all exploits used in the wild.[32] Exploits for N-day vulnerabilities are often embedded in exploit kits and tools sold or rented in the underground markets, ranging from a few hundred to a few thousand dollars, depending on exploit reliability and the adopted exploit portfolio.[33] AaaS and private groups are known to perform to at least some extent autonomous vulnerability research and exploit development, as well as to acquire zero days and related exploits from other private actors in the semi-regulated market. This can be seen through private sector zero day vendors like Zerodium,[34] as well as the Israeli NSO Group: Both organizations likely house their own vulnerability research teams while also purchasing outside exploits. The market may also play the role of a catalyst to favor the transfer of these capabilities across actors: Vulnerability researchers selling vulnerabilities and exploits to AaaS groups may later be hired and integrated in the AaaS group itself. Similarly, internal capabilities may "spin-off" externally to a new or existent vulnerability research company. Similar dynamics have been observed, for example, for NSO Group.[35]

Novel and effective offensive capabilities offered from free-access underground markets are almost nonexistent.[36] These markets are largely populated from scammers targeting wannabe criminals, resulting in an untrustworthy field for trade.[37] Vulnerability research remains relatively basic in these markets, and appears to rely mainly on preexistent technologies or automated frameworks (e.g., to find low-hanging-fruit vulnerabilities).[38] Pull-in markets are generally unable to supply new vulnerabilities and exploits, which are reserved for the more elite spaces of segregated forums and marketplaces where appropriate trust mechanisms enabling their trade are in place.[39] In this respect segregated markets, built on reliable trust mechanisms and user verification, can provide both room for discussions between members, cooperation and research, and the trade of highly effective products and services resulting also from private groups.[40] These markets may trade zero day vulnerabilities weaponized in ready-to-deploy exploits. By contrast, pull-in markets have proved able to supply new malware payload generation techniques and to make progress in the management of more complex command-and-control architectures.[41]

[32] Jay Jacobs, Sasha Romanosky, Idris Adjerid, and Wade Baker, "Improving Vulnerability Remediation through Better Exploit Prediction," WEIS, 2009, https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf.

[33] Boris Larin, "Magnitude Exploit Kit – Evolution," *Kapersky SecureList,* June 24, 2020, https://securelist.com/magnitude-exploit-kit-evolution/97436/.

[34] "Program Overview," Zerodium, accessed January 19, 2021, https://zerodium.com/program.html.

[35] 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/.

[36] Ibid.

[37] Cormac Herley and Dinei Florencio, "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy," *Microsoft Research*, June 2009, https://www.microsoft.com/en-us/research/publication/nobody-sells-gold-for-the-price-of-silver-dishonesty-uncertainty-and-the-underground-economy/.

[38] Luca Allodi, "Economic Factors of Vulnerability Trade and Exploitation," In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (2017): 1483-1499.

[39] Allodi et al., "Then and Now"; Krebs, "Why Were the Russians So Set against This Hacker Being Extradited?"

[40] F. Wehinger, "The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services," IEEE, 2011.

[41] M. Campobasso and L. Allodi, "Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale," CCS '20: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020; Allodi, "Economic Factors of Vulnerability Trade and Exploitation."

PILLAR TWO:
Malware Payload Development

The most common part of a malware-oriented campaign is the malware itself. This pillar includes any malware or malware tools written or used by attackers to conduct offensive cyber operations, or any forum that encourages or conducts exchanges of malware.

Malware generally comprises the bulk of OCC proliferation debates. Malware can be openly shared as offensive security and intrusion tools,[42] developed and sold as stalkerware,[43] or even licensed as commercial spyware to large organizations. Free intrusion tools can be found on code-sharing sites and are regularly developed within the cybersecurity community, although many target older systems, or exploit weaknesses that result from common developer or user errors.

Malware can also be found within underground marketplaces. Within these, malware varies widely in its ultimate desired effect, how effectively it evades detection, and how it encrypts its outgoing and incoming communications. This is largely correlated to the quality—or maturity—of the underground market itself.[44] In self-regulated spaces, rules on reselling software or selling unreliable software can be strictly enforced for more mature markets, and a rules violation often results in permanent expulsion from the community. In these marketplaces, it is relatively common to see malware advertised for "exclusive" trade to a limited number of buyers, usually at a higher price tag than other non-exclusive malware.[45]

Malware payloads become more tailored and effective for more exclusive marketplaces, especially for the most exclusive of clients: government organizations. Government agencies incapable of developing their own OCC recur to AaaS groups to obtain high-quality malware to conduct their offensive campaigns; this malware can rely on 0days and sophisticated stealth mechanisms to conduct offensive cyber operations. The cybersecurity industry has a long-held belief in the Digital Quartermaster theory with regard to Chinese APTs: that malware similarity among multiple Chinese threat groups suggests that there exists an organization within the Chinese government writing and disseminating malware to multiple operational units.[46] In addition, Vault7 and other information shared via Wikileaks alleged that the United States' National Security Agency[47] and Central Intelligence Agency[48] each have their own centralized OCC development groups. Most recently, the US Treasury Department sanctioned a Russian state research center (TsNIIKhM) for writing malware linked to Russian cyber operations in the Middle East.[49]

If state-backed malware in a government is not constructed in-house, contractors may also fill that void. Contractors and other Access-as-a-Service firms that provide malware development services allow governments to purchase capabilities they may not be able to build in-house themselves. For example, in November 2016, researchers asserted that Boyusec, the company behind Chinese espionage group APT3, and Huawei, a company currently embroiled in commercial espionage allegations, were jointly producing a backdoor in Chinese-made telecom equipment for Chinese intelligence.[50] Similarly, AaaS groups such as the NSO Group develop in-house malware that is then provided as an additional capability to

[42] "Security Tools," GitHub, accessed January 19, 2021, https://github.com/topics/security-tools?q=red+team&unscoped_q=red+team.

[43] Damien Wilde, "Google Removes Seven Major Stalkerware Apps from the Play Store," 9 to 5 Google, July 18, 2019, https://9to5google.com/2019/07/18/stalkerware-apps-play-store/.

[44] "Multiple vs. Exclusive Sales on the Dark Web: What's in a Sale?" *Digital Shadows*, June 29, 2020, https://www.digitalshadows.com/blog-and-research/multiple-vs-exclusive-sales-on-the-dark-web/.

[45] Of course, whether these contracts are eventually breached by the seller is very hard to measure. Forum moderation and escrowing can play an important role here, where forum administrators become "guarantors" for both the single transaction and the longer-term contract enforcement.

[46] "Supply Chain Analysis: From Quartermaster to SunshopFireEye," *Security Reimagined*, 2014, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf.

[47] Lorenzo Franceschi-Bicchierai, "Who Are the NSA's Elite Hackers?" *Vice*, August 23, 2016, https://www.vice.com/en_us/article/bmvyxw/nsa-hacking-unit-tao-cyberwar.

[48] Sean Gallagher, "Helpful(?) Coding Tips from the CIA's School of Hacks," *ARS Technica*, March 8, 2017, https://arstechnica.com/information-technology/2017/03/malware-101-the-cias-dos-and-donts-for-tool-developers/.

[49] "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware," US Department of the Treasury, October 23, 2020, https://home.treasury.gov/news/press-releases/sm1162.

[50] Catalin Cimpanu, "Chinese Government Contractor Identified as Cyber-Espionage Group APT3," *Bleeping Computer*, May 18, 2017, https://www.bleepingcomputer.com/news/security/chinese-government-contractor-identified-as-cyber-espionage-group-apt3/; Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service," *Washington Free Beacon*, November 29, 2016, https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/.

inquiring governments; NSO's Pegasus malware is known for its modularity and relative sophistication, adopting multistage infection stages to maintain (and increase chances of) persistence on the system. This is generally achieved by adopting multiple exploits and so-called droppers, which are responsible for maintaining persistence on the system and may be used to customize malware functionalities after installation, for example, by installing or updating malware modules. Other techniques rely on the employment of stealthy malware, such as rootkits, to maintain persistence on the infected system; for example, part of the offering from Hacking Team was VectorEDK, a Unified Extensible Firmware Interface (UEFI) malware ensuring that, even if the second-stage malware is detected and removed, the underlying UEFI infection remains and can be used to reinstall the wiped malware at the attacker's will.[51] Similar multistage techniques are used by hackers operating in the underground markets, for example, to provide pay-per-install (PPI) services.

PILLAR THREE:
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, virtual private network (VPN) services, or delivery accounts involved with the initial creation of an offensive cyber operation.

An offensive cyber operation usually consists of more than just malware payloads and exploits. Malicious software needs to be delivered and, in most cases, communicated with. The initial delivery, command and control, and final exfiltration all depend on reliable infrastructure set up by the attacker. This is well known as the "infrastructure" segment of the Diamond Model of Intrusion Analysis, a popular model to analyze and track the characteristics of cyber intrusions.[52] OCC infrastructure can consist of command-and-control servers, domain names of phishing pages, resources to launch phishing attacks (e.g., leaked email addresses for phishing emails), or abused technologies (ranging from software within a company's supply chain to mass-mail providers).

In many state-sponsored cases, infrastructure for offensive cyber operations often compromises or otherwise abuses legitimate internet technologies, largely to cover indicators of malicious activity. In 2015, Chinese threat actor group Deep Panda used VPN services to conduct cyber espionage campaigns.[53] Many of the VPN endpoints used in the campaign were also found to be compromised machines belonging to non-Chinese companies, further obscuring the source of network traffic.[54] State-sponsored cyber operations have also compromised legitimate websites to serve malware.[55] From a command-and-control perspective, nation states[56] and cybercriminals[57] alike have developed malware that uses legitimate cloud services like Google Drive to communicate with or download additional malware onto victim machines.

Particularly in self-regulated markets, setting up and running command-and-control infrastructure for malware campaigns is at constant risk of law enforcement takedowns. To prevent unwanted interruptions to their illegal enterprises, criminal communities will often purchase "bulletproof" hosting services, which provide infrastructure resistant to intervention from regulators or law enforcement.[58] These services can be created by criminals themselves,[59] or individuals residing in countries with fewer restrictions. Providers of these bulletproof hosting services are abundant on criminal forums. In providing such services, underground markets play an important role in the supply of related infrastructural services. Some of the services are built off of infrastructure yielded from previous offensive operations (e.g., botnets obtained from phishing campaigns). AaaS and private actors are known to deploy their infrastructure globally to enable activities in different countries, particularly to

[51] Andy Greenberg, "A China Linked Group Repurposed Hacking Team's Stealthy Software," *Wired*, October 5, 2020, https://www.wired.com/story/hacking-team-uefi-tool-spyware/.

[52] Sergio Caltagirone, Andy Pendergast, and Chris Betz, "The Diamond Model of Intrusion Analysis," *Semantic Scholar*, 2013, https://pdfs.semanticscholar.org/dca1/9253781fbc429d85ec09e8f0f7f2ddbe7fdf.pdf?_ga=2.66524334.1838484345.1597299841-2110084014.1597299841.

[53] "Chinese VPN Service as Attack Platform?" *Krebs on Security*, August 4, 2015, https://krebsonsecurity.com/tag/terracotta-vpn/.

[54] Peter Beardmore, "An Update on Terracotta VPN," *RSA*, April 1, 2016, https://www.rsa.com/en-us/blog/2016-04/an-update-on-terracotta-vpn.

[55] Matthieu Faou, "OceanLotus: New Watering Hole Attack in Southeast Asia," *We Live Security*, November 20, 2018, https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/.

[56] Tara Seals, "RogueRobin Malware Uses Google Drive as C2 Channel," *Threatpost*, January 23, 2019, https://threatpost.com/roguerobin-google-drive-c2/141079/.

[57] "The Tetrade: Brazilian Banking Malware Goes Global," *Kapersky SecureList,* July 14, 2020, https://securelist.com/the-tetrade-brazilian-banking-malware/97779/.

[58] "What Is Bulletproof Hosting?" Norton, 2020, https://us.norton.com/internetsecurity-emerging-threats-what-is-bulletproof-hosting.html.

[59] "German Cops Raid 'Cyberbunker 2.0,' Arrest 7 in Child Porn, Dark Web Market Sting," *Krebs on Security*, September 28, 2019, https://krebsonsecurity.com/2019/09/german-cops-raid-cyberbunker-2-0-arrest-7-in-child-porn-dark-web-market-sting/.

maintain the command-and-control activities associated with the service those actors provide; in at least one previous case, that of DarkMatter (a UAE actor employing US mercenaries in so-called Project Raven),[60] an AaaS group attempted to become a trusted Certification Authority—a position that would have allowed the group to sign as trusted command-and-control servers, potentially allowing them to distribute software as part of their offensive operations.

Either way, it is highly likely that nation states, criminals, or any other entities that set up technical infrastructure for offensive cyber operations do so in bulk. In self-regulated markets, fake social media or email account creation[61] for spam, false reviewing, and other related fraudulent activities are a booming business, as are the associated captcha-breaking services and dedicated hardware products associated with creating the accounts.[62] For organizations that do their setup in-house, many individuals that set up infrastructure for operations often follow a pattern when doing so. For example, the Chinese actors behind the US Office of Personnel Management hack used Marvel superhero themes[63] when setting up their domains.

PILLAR FOUR: Operational Management

A 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 conducting cyber operations.

Malware, exploits, and associated infrastructure do not proliferate themselves. Forming strategic direction, establishing organizational processes, building relationships, and developing contingency plans all require people and all need to be developed, executed, and iterated for any offensive cyber operation organization's overall success.

Creating processes and directing individuals to carry out specific portions of an operation is common even in small cyber criminal firms. The unsealed US Department of Justice

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

[61] "Fake Account Creation: It's Fraud by Any Other Name," *Cequence*, July 2019, https://www.cequence.ai/blog/fake-account-creation-its-fraud-by-any-other-name/.

[62] Ting Fang Yen, "How to Register Millions of Fake Accounts with Ease," *Datavisor*, September 29, 2015, https://www.datavisor.com/blog/how-to-register-millions-of-fake-accounts-with-ease/.

[63] "OPM Breach Analysis," *ThreatConnect*, June 5, 2015, https://threatconnect.com/blog/opm-breach-analysis/.

indictment of Andrey Turchin,[64] a member of cybercriminal group FXMSP,[65] revealed that the group followed a repeatable process: using phishing emails or brute-forcing credentials to get into corporate networks, deploying malware to establish persistence within the networks themselves, and then monetizing the access based on level of access and victim entity on multiple criminal forums. To monetize the access, Turchin allegedly hired fellow cybercriminal Antony Moricone (or “BigPetya”)[66] as his sales manager for this process.

Other criminal operations are supported by (and scaled through) well-devised criminal business models. In 2020, Mr. Moricone’s job had since been automated through the creation of Impersonation-as-a-Service (IMPaaS) infrastructure,[67] another example of criminal innovation in response to the problem of how to monetize stolen information with less manual effort. The IMPaaS model creates a whole supply chain of products originating from systematic malware infection, pushing user information (e.g., credentials, system fingerprints, web cookies) to the systems of paying customers selecting their products in an e-commerce-like market when malware collects updated information.

Creating a high-functioning state-sponsored department for OCC requires far more organizational knowledge than that of a small cybercrime group. Departments that house offensive cyber capabilities must know how to collect intelligence on targets, tailor operations for those targets, and execute operations with success. The knowledge and processes inherent to these departments can be homegrown through years of in-house research and development but turning manual processes into a collective, automated effort requires skill, nonlinear input of time, and no small effort. Witness the work of the US Defense Advanced Research Projects Agency to automate many manual processes within vulnerability discovery and patching through its Cyber Grand Challenge program.[68] While more of a defensive example than one strictly related to OCC, the Cyber Grand Challenge is a form of research and development that could influence future processes within OCC in the US government.

Such departments can also be assisted by an outside organization. For example, the UAE’s cyber surveillance organization Development Research Exploitation and Analysis Department (DREAD) was initially created in 2008, assisted by an outside organization. Former US counterterrorism coordinator Richard Clarke recommended that the UAE create a cyber surveillance agency, then helped create and mature the organization through his own company, Good Harbor Consulting, until 2010.[69] Good Harbor did this by creating the overall structure of the organization, and hiring US subcontractors well versed in offensive cyber operations to develop the project’s necessary covert computer networks, and necessary training for potential Emirati staff.[70]

Cyber capabilities can be further supplemented with third-party vendors. The UAE moved to expand DREAD capabilities with the help of other contractors like US firm Cyberpoint, whose famous Project Raven effectively introduced UAE operatives to espionage techniques they later used on both domestic dissidents and US citizens.[71] 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.[72]

[64] Indictment, United States v. Andrey Turchin, 2:18-cr-00303-RAJ (United States District Court for the Western District of Washington at Seattle, December 12, 2018), https://www.justice.gov/usao-wdwa/press-release/file/1292541/download.

[65] Charlie Osborne, “Fxmsp Hacker Indicted by Feds for Selling Backdoor Access to Hundreds of Companies,” *ZDNet*, July 8, 2020, https://www.zdnet.com/article/fxmsp-hacker-indicted-by-feds-for-selling-network-access-impacting-hundreds-of-companies/.

[66] Tara Seals, “Notorious Hacker ‘Fxmsp’ Outed after Widespread Access-Dealing,” *Threatpost*, July 8, 2020, https://threatpost.com/notorious-hacker-fxmsp-outed/157275/.

[67] Michele Campobasso and Luca Allodi, “Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale,” In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (September 9, 2020): 1665-1680, https://arxiv.org/abs/2009.04344.

[68] Dustin Fraze, “Cyber Grand Challenge,” Defense Advance Research Projects Agency, US Government, https://www.darpa.mil/program/cyber-grand-challenge.

[69] 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-idUSKBN1YE1OB.

[70] Ibid.

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

[72] Ibid.

PILLAR FIVE:
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 between them that facilitate the growth of OCC.

Organizations cannot spontaneously generate skilled teams for offensive cyber operations. Operators, vulnerability researchers, and malware authors must be provided with the proper training to do their jobs, while new employees must be oriented, trained, and overseen.

As with other pillars, offensive training programs can be offered for defensive reasons. Training on open source security tools like Nmap and Metasploit and other tools within Kali Linux are widely available on YouTube, advertised as "ethical hacking" courses.[73] Certifications like the Offensive Security Certified Professional, alongside its associated training and workbooks, are conducted by companies like Offsec Services LTD.[74] Some of these certifications are not only desired experience for top-tier penetration testing, auditing, and consulting job applications, but can also be prerequisites to apply.[75] Many security conferences, ranging from the widely attended BlackHat conferences[76] to more tailored offensive security conferences like INFILTRATE,[77] also provide training sessions that develop the offensive security community (although members of US and other intelligence agencies also likely attend the same conferences).

Training also exists for offensive cyber operations (albeit in less open venues). Underground criminal forums contain explicit fraud tutorials[78] showing how to turn dumps of stolen credit card numbers into Bitcoin, and provide setup guides for commodity malware sold on those forums.[79] These tutorials and malware instructions are, in essence, "replication guides" to set up or re-create malware configurations. Some tutorials are provided together with "kits" (e.g., phishing kits) that any attacker can deploy and readily use against their targets. This is also common in the private sector: The organization that created Cobalt Strike, a popular penetration testing tool also used frequently in APT attacks,[80] hosts free video tutorials[81] on how to use the tool.

Organizations offering offensive cyber operations training in the semi-regulated space will go out of their way to travel to foreign jurisdictions, providing their services to government officials and organizations in exclusive workshops. Governments have a myriad of sources to pull from when deciding to train their employees in offensive cyber operations tactics and techniques. In-house solutions developed by governments, such as the National Security

[73] freeCodeCamp.org, Linux for Ethical Hackers (Kali Linux Tutorial), YouTube, July 5, 2019, audiovisual recording, 1:27, https://www.youtube.com/results?search_query=kali+linux+tutorial.

[74] "Penetration Testing with Kali Linux (PEN-200)," Offensive Security, accessed January 19, 2021, https://www.offensive-security.com/pwk-oscp/.

[75] "Penetration Testing with Kali Linux (PEN-200)," Start a Cyber Career, accessed January 19, 2021, https://startacybercareer.com/oscp-worth-it-cost-comparision-benefits/#benefit.

[76] "Training Schedule," Black Hat USA, 2020, https://www.blackhat.com/us-20/training/schedule/listing.html.

[77] "Training," INFILTRATE, accessed January 19, 2021, https://www.infiltratecon.com/conference/training.html.

[78] Winnona Desombre and Dan Byrnes, "Thieves and Geeks: Russian and Chinese Hacking Communities," *Recorded Future*, October 10, 2018, https://www.recordedfuture.com/russian-chinese-hacking-communities/.

[79] INSIKT Group, "Bestsellers in the Underground Economy: Measuring Malware Popularity by Forum," *Recorded Future*, July 24, 2019, https://www.recordedfuture.com/measuring-malware-popularity/.

[80] "Multi-stage APT Attack Drops Cobalt Strike Using Malleable C2 Feature," *Malwarebytes Labs*, June 17, 2020, https://blog.malwarebytes.com/threat-analysis/2020/06/multi-stage-apt-attack-drops-cobalt-strike-using-malleable-c2-feature/.

[81] "Training," Cobalt Strike, accessed January 19, 2021, https://www.cobaltstrike.com/training.

Agency's National Cryptologic School,[82] have historically been useful in developing tailored expertise. Additionally, education budgets exist to supplement additional learning initiatives: For example, the US Scholarship for Service program allows individuals in STEM (science, technology, engineering, and mathematics) to receive a full-ride scholarship to accredited schools in exchange for government service. Similarly, cybersecurity training curricula are developed by associations such as the Association for Computing Machinery and IEEE in joint task forces involving members from multiple institutions.[83]

Ultimately, organizations that offer trainings, especially those designed for government audiences, do not provide just technical expertise. By putting people in a room together, they create the connective tissue between individuals and organizations necessary to conduct offensive cyber operations. Naturally, the specific type of training provided by different entities also depends on the business models or incentives motivating these actors in providing the training. For example, AaaS or private groups in general may be interested in providing training for the deployment or employment of their own technology (something well exemplified in the Hacking Team's leaks, for example), but less so in providing training to third parties for the development of those offensive capabilities. However, governments may adopt or support a series of training schemes also aimed at generating and selecting the talent they intend to acquire down the line.

ZEROING IN ON OFFENSIVE CYBER CAPABILITY COUNTERPROLIFERATION

Counterproliferation policy options in cyberspace are underutilized by the United States primarily due to a narrow view of "cyber weaponry" versus underlying cyber capability. Understanding cyber proliferation as the proliferation of multiple capabilities gives policy makers enough granularity to begin crafting technically feasible counterproliferation policies.

Understanding the way that criminal markets, governmental agencies, and private AaaS groups offer and build state-of-the-art products for conducting offensive cyber operations also allows policy makers to target a specific subset of actors without damaging the cyber security industry as a whole. Specifically, uncovering the role AaaS groups play in proliferating offensive cyber capabilities will help drive more effective counterproliferation policy in the United States, the EU, and elsewhere. We expand on the ways AaaS groups proliferate cyber capabilities in our companion piece, *Countering Cyber Proliferation: Zeroing in on Access as a Service*. Focusing on policing the behavior of Access-as-a-Service providers, exploit vendors, and other offensive cyber training organizations that deliberately reach out to adversary governments (especially governments that have strategically prioritized targeting the United States in cyberspace) would create swift and beneficial results for ensuring that adversaries do not get a private sector advantage when attacking the United States and its allies.

[82] "Defense Language Institute and National Cryptologic School Agreement Helps U.S. Service Personnel Earn Associate Degree," NSA CSS, June 12, 2019, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/1874058/defense-language-institute-and-national-cryptologic-school-agreement-helps-us-s/.

[83] "ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline," CSEC 2017, 2017, https://cybered.hosting.acm.org/wp/.

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.

Michele Campobasso is a PhD candidate at the Security Group of Eindhoven University of Technology under the supervision of Dr. Luca Allodi. 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.

Dr. James Shires is an Assistant Professor at the Institute for Security and Global Affairs, University of Leiden. 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.

Robert Morgus is a Senior Director for the US Cyberspace Solarium Commission, where he directs research and analysis for Task Force Two. His research interests include focuses on mechanisms to counter the spread of offensive cyber capability, cybersecurity and international governance, Russian internet doctrine, international cybersecurity norms, internet governance, cybersecurity insurance, amongst others.

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?

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.

Atlantic Council Board of Directors

Atlantic Council

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

Atlantic Council

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

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