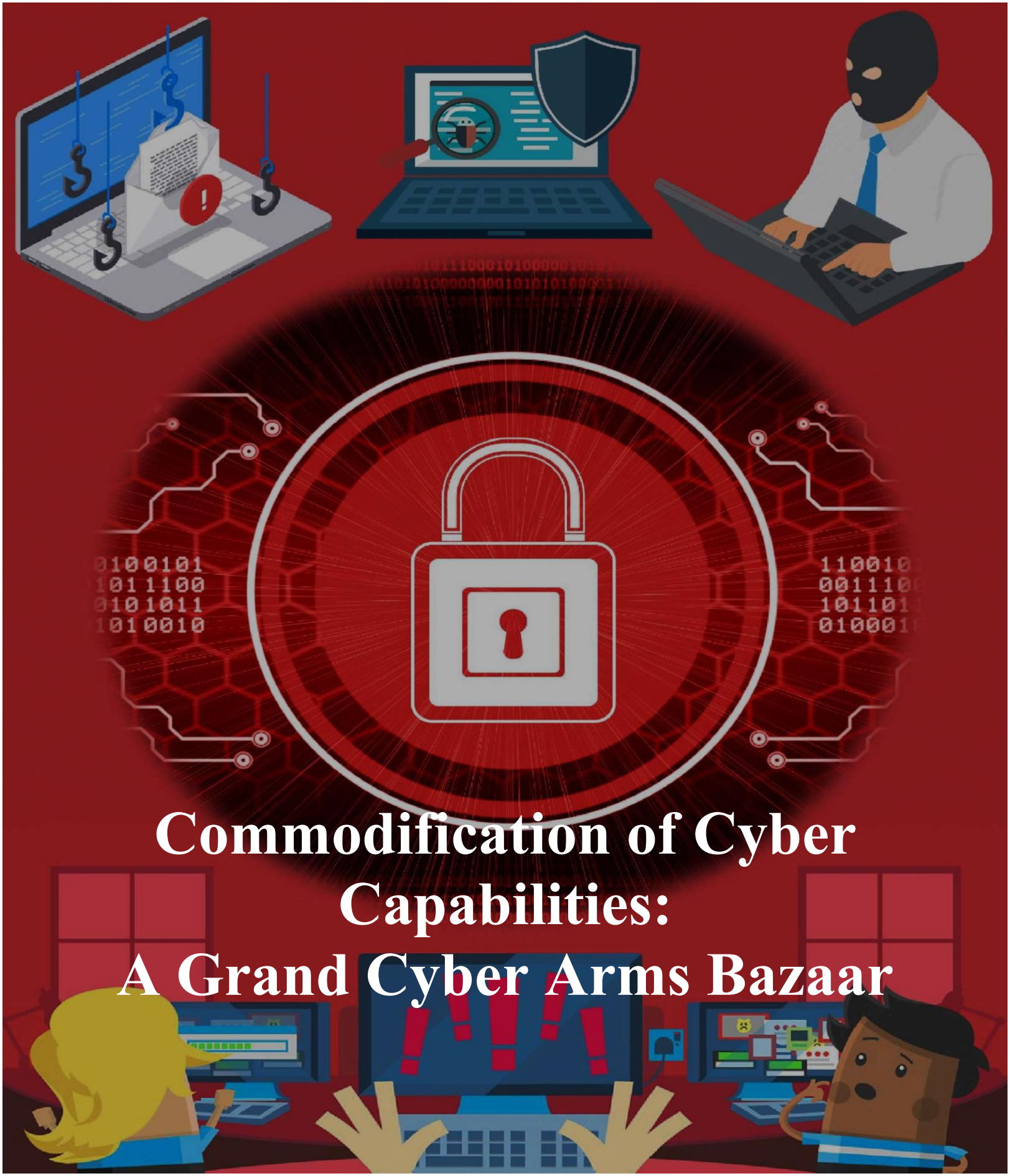


Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar

2019 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Table of Contents

Page

Executive Summary

A proliferation and commodification of cyber offensive capabilities is reshaping the cyber balance of power, enabling an expanded array of actors to use cyber for geopolitical impact or economic gain. From the use of offensive cyberattack by nation-states directly against another or by co-opting cyber criminals, this trend has blurred the line between spies and non-state malicious hackers.

An expanding array of new entrants - both nation-states and non-state actors - with significant capabilities is reshaping the cyber threat landscape. The tools at their disposal allow for unprecedented espionage and surveillance capabilities, which often are the precursors for criminal financial gain, destruction, and disruption operations. Just as the vulnerability surface for cyber is marked by being mostly civilian infrastructure, so increasingly are we seeing non-state actors, including commercial entities, building capabilities that years ago were solely held by a handful of state actors.

The proliferation of cyber tools, which are hard to control and contain, is lowering the barriers to entry. The ability to buy capabilities off the shelf, to bridge gaps in capabilities, or to build tailored tools organically ensures the complex dynamics of the current cyber threat landscape will continue to challenge national security, the commercial sector, and civilians, particularly, vulnerable populations.

The increasing ability to buy cyber tools on a commercial basis allows both nation-state and non-state actors to leapfrog by crossing the line from emerging threat to an established threat quickly; thus leapfrogging is seen as a key driver in the cyber threat landscape. When combined with the challenges of definitive and timely attribution, a threat actor that emerges quickly could inject a high level of geopolitical instability into a conflict that would be more difficult to anticipate than traditional military changes in the balance of power, such as acquisitions of new weapons.

One challenge that government and private sector executives will face in the current environment is how to posture their organization to minimize surprise around the emergence of new cyber actors and effects. In this paper, we present a framework for understanding the sophistication of threat actors in a threat landscape that is characterized by a "grand cyber arms bazaar" in which sophisticated cyber capabilities are widely available from commercial, criminal and open sources.

Our framework includes three distinct categories of sophistication:

1. Established actors—those with the most advanced, accurate, and agile tools.

2. Emerging actors—which include nation-states, criminal organizations, and those with defined processes.

3. Opportunistic actors—generally those associated with cybercriminal activity. An important differentiator in the three categories of this framework of sophistication is motivation.

Whether it is financial gain, collection and surveillance, or offensive attack, cyber actors at each level of sophistication are able to carry out impactful cyber campaigns. Through three case studies, we apply the framework to determine the level of cyber sophistication of nation-state actors.

Because of its geopolitical position in the world and its considerable and vulnerable attack surface, the West faces particular challenges in addressing the cyber threat and several issues exacerbate an already problematic environment including an inconsistent ability to hold actors responsible. Among the key issues that may need to be addressed are the lack of clear redlines that set expectations and implications for the use of cyber weapons by state and non-state actors. Another consideration is the evolving understanding of how escalation and unintended consequences can and should be managed in a cyberattack. Overall, as would be expected from a relatively new area of warfare, the rules of engagement are still emerging and unclear.

This paper explores two potential types of futures. The first are situations of rapid escalation — which might emerge when the geopolitical environment is lacking consensus or broadly held norms for acceptable behavior, just as cyberattack capabilities are becoming more powerful and not well understood. A second future scenario we see as likely is the foundation of an inflection point. In this scenario, enough actors share a perception that an inflection point has been reached, and begin to take steps to control or manage the evolution or revolution in this sphere.

Cyber Threat Landscape: More Actors, Capabilities, and Connectivity

The modern cyber threat landscape is distinguished by an expanding array of state and non-state actors with access to various cyber tools or weapons, which may be combined to conduct advanced operations aimed at collection, criminal financial gain, or digital surveillance. Nation-states view cyber espionage as a tool for countering internal dissent or acquiring diplomatic or competitive advantage. Some governments use cyber asymmetry to challenge established powers with significant diplomatic sway or military power or to target private sector entities - a tactic which can be difficult to address with diplomatic or military means. Others have latched onto financially motivated cybercrime as a means of evading sanctions.

- Non-state actors, such as cyber criminals, exploit an increasingly interconnected environment to mount sophisticated cyber operations that can yield vast sums from targeted financial institutions or from large scale ransomware campaigns against smaller targets. These actors may also sell their malware and skills “as a service” in online forums, including on the dark web.

- In some cases, state actors may sponsor or co-opt indigenous cyber criminals, hacktivists, or semi-professional criminal hackers to either launch cyber operations with a veneer of deniability or quickly draw upon foreign technical expertise.

The cyber environment is also characterized by a low entry barrier for new actors, as cyber tools are hard to contain and control. Code is nearly impossible to regulate and cyber actors are selling or sharing their capabilities and techniques without restraint. Absent regulation, automation and proliferation of sophisticated and "usable" cyber tools abound. As a result, malicious actors can now embark on opportunistic attacks that are also sophisticated.

- A recent dynamic is the diffusion of expertise as former government, intelligence, or military cyber experts offer their expertise for hire to nation-states seeking to jump-start cyber programs. The government of the United Arab Emirates (UAE) hired former US government intelligence personnel working for Dark Matter to build an advanced capability to compromise challenging technical targets and boost the government's cyber abilities. The contractors, Dark Matter, may have operated at a level close to top-tier national security agencies, thus boosting the UAE's cyber abilities significantly and quickly to achieve previously hard-to-obtain goals in cyberspace.

In other cases, commercial firms have offered sophisticated cyber capabilities for sale to foreign governments, or customers with close ties to an unstable military regime that may use it against an adversary or its own citizens.[1] For example, FinFisher, a private company based in Germany, developed a capability that has been widely used and exported. According to Citizen Lab, there have been "33 likely government users of FinFisher in 32 countries."[2,3]

Below (Table 1) are examples of similar operations with wide-ranging impact:

[1] In addition to DarkMatter, NSO Group and FinFisher, this research revealed several other firms competing in this space: Verint, Interionet, Gamma Group, Intellexa, Black Cube, CyberPoint International, Senpai Technologies, Al-Thuraya Consultancy & Research, Omniscope Limited, Q Cyber Technologies, and SecureTech.

[2] Marczak, Bill, John-Scott Railton, Adam Senft, Brene Poetranto, Sarah McKune (2015, October 15). Citizen Labs. *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation.* Retrieved from https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#2

[3] Mazzetti, Mark, Adam Goldman, Ronen Bergman and Nicole Perlroth (2019, March 21). New York Times. *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments.* Retrieved from https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html

Table 1: Cyber Operations and Impact

Operation	Severity	Scale	Duration	Specific
NotPetya	High: data destruction	Global. Affected organizations in Europe, the US and Asia (Maersk, Merck, Rosneft, Beiersdorf, DHL and others) but also a concentration in Ukraine (banking, nuclear power plants, airports, metro services).	Short-term, with recovery spanning over months to a year.	No
WannaCry	High: data destruction	Global, but primarily in Russia, Ukraine, India and Taiwan. Operation affected multinationals, critical infrastructure and government.	Short-term, with recovery spanning over months to a year.	No
Destover	High: data destruction	Focused on Sony Pictures Entertainment (<7,600 employees), a subsidiary of Sony Corporation (131,700 employees in 2015).	Short-term, with recovery in months.	Yes
Stuxnet	High: destruction of centrifuges	Focused on Iran's nuclear weapon development program.	<1 year	Yes
Various offensive cyber operations against ISIS by US, Australia, UK	Varied: some data destruction but also denial and manipulation effects	Focused on Islamic State.	Unknown	Yes

A major contributor to the dynamic global threat landscape is the pace of technological evolution, which is marked by growing interconnectivity. This interconnectivity not only provides a larger attack surface in general, but also expands the reach to a growing set of cyber threat actors. Internet of Things (IoT) devices are an instrumental example. Actors can compromise these devices all over the world, directing them to carry out an attack that is both large in scale and difficult to attribute given how dispersed the actors are. As with much of new technology, the regulatory environment that constructs a framework for safe and effective use often lags behind, leaving otherwise innocuous devices susceptible to exploitation.

In some cases, threat actors looking to take advantage of technological innovations to expand or improve operations may not fully understand how their activity will have a geopolitical impact. These threat actors may be ignorant of potential consequences or the "domino effect" inherent in such an interconnected environment. Many organizations do not own all of their infrastructure, but use subcontractors and shared service providers instead. Actors may not realize, or not care, if malicious code meant for one target spreads to others, or if a similarly financially motivated attack disrupts a nation's critical infrastructure sector.

The ability of organizations and individuals to patch their systems has failed to keep pace with fast-increasing numbers of devices and connectivity, new applications of technology, and the speed with which threat actors can find and exploit vulnerabilities. Many of the experts interviewed for this project shared similar concerns about the software architectural design process being fundamentally flawed and therefore more difficult to defend.

The combination of more cyber actors with access to similar tools and fast-evolving technology likely will make it increasingly difficult to distinguish threat actors from each other and from legitimate network activity. Actor motivations are blurrier and their tactics, techniques, and procedures (TTPs) are not always indicative of their targets. For example, as a defense contractor one may assume that the target of a cyberattack would be access to the US Department of Defense's secure systems; however, nefarious actors may be just as interested in acquiring employees' personally identifiable information (PII) for fraudulent activities. It is also possible that cyber experts, including former government or military personnel, may not understand the intent of nation-state actors who hire them or they may choose to turn a blind eye until they have become embroiled in an ethically questionable cyber campaign.

Common Approaches to Acquiring Cyber Capability: Buy, Build, Bridge

Based on interviews with experts in academia, industry, and government, we identified three approaches used by threat actors to acquire cyber capabilities: create an indigenous capability, buy a capability from external sources, or use partnerships and purchase as a "bridge" to eventually developing custom capabilities. These strategies likely will remain viable over the long term, continuing a trend of access to capability by an increasing number and range of threat actors. In particular, the ability to buy or bridge capabilities will continue to offer actors with limited skills

opportunities to achieve asymmetric advantage. We also assess that sophisticated actors will find value in an expansion of the cyber marketplace and diffusion of cyber tools and capabilities.

Buy: A key evolutionary driver of this diverse landscape is the ability for actors, nation-states and otherwise, to purchase their capabilities, enabling "leapfrogging." Theoretically, leapfrogging allows an actor who is initially categorized as an emerging threat to become an established threat, assuming the actors also are able to acquire the products, processes, and people to accompany those tools. For actors that purchase their tools, there are tools with high barriers and those with low barriers:

- Some purchased tools may offer a low barrier for the expertise and tradecraft required to employ them. Such tools are often inexpensive, easily customizable, and readily available on the open market. These "off the shelf" tools are easily commoditized and sold in marketplaces.

- Other tools may require significant financial and personnel resources and operational tradecraft to employ. They may be designed to achieve a specific and reliable effect against a specific target in a way that advances an actor's geopolitical aims.

- While on the surface, tools with high barriers to entry appear to be the most significant threat, experts in the field warn of the dangers associated with low barrier tools. One expert explicitly noted that it is easy for any actor to use a low barrier tool to cast an unspecific effect at any point in time if their goal is not precision, and there are little to no concerns for collateral damage.

The increasing availability of anonymous marketplaces and information exchanges enables efficient collaboration and rapid exchange of information around new tools and exploits. These forums will not dissipate- even after several attempts by law enforcement to curb underground fora and marketplaces, notably, the takedowns of AlphaBay and Hansa in 2017. Despite law enforcement's best efforts, criminals continue to purchase tools and capabilities for conducting cyberattacks.[4] Proliferation of capabilities by way of transaction is the new normal. In addition to established marketplaces for trading cyber tools and tradecraft, the rise of secure channels such as Telegram and Discord further establishes this culture of commoditizing cyber capabilities, facilitating private transactions or exchanges of stolen data, malicious code, or hacking for hire.

Bridge: Aside from purchasing "ready to go" tools or capabilities, actors can also accelerate the acquisition of cyber capabilities and bridge cyber gaps by leveraging the tools and resources of another organization through a partnership. When trying to achieve geopolitical outcomes, for

[4] Van Wirdum, Aaron (2019, January 31). Bitcoin Magazine. *Chainalysis: Darknet Market Activity Nearly Doubled Throughout 2018*. Retrieved from https://bitcoinmagazine.com/articles/chainalysis-darknet-market-activity-nearly-doubled-throughout-2018

example, experts identify two types of partnerships that can be drivers for proliferation of capabilities: partnerships with other nation-states and with criminal or private organizations. A partnership between nation-states can expedite the development of capabilities in the lower-tier partner. One expert in the field emphasized that we particularly see this happening surrounding the development of spheres of influence.

Partnerships with criminal or commercial firms (e.g., Dark Matter and NSO Group) provide an avenue for individuals, companies, or nation-states to purchase a broad range of capabilities. Reuters journalists uncovered a partnership between Dark Matter and the UAE government that also utilized American cyber mercenaries and whose mission was to spy on human rights activists, journalists and political rivals.[5]

Build: While some nation-states elect to purchase their tools and capabilities, those that choose to build their own defensive and offensive capabilities are more likely to be categorized in a higher tier given the sophistication and precision needed to create and use these tools effectively. One academic expert opined that nations seeking to incorporate cyberattack into their military capabilities would eventually seek to develop indigenous capabilities, rather than rely on external sources. Several factors shape the level of indigenous capability that a nation may achieve. Indigenous technical talent is a key factor.

Other Factors: The ability to create organizations and processes that blend operators, developers, analysts, strategists, and even a legal department to conduct operations and manage risk is paramount in developing a robust and sustainable capability. Even a strong network and operational infrastructure from which to operate is key. Infrastructure is important not only for the development of capabilities from which to build and launch attacks, but also, for the defense against external threats. Additionally, a nation-state's political, economic, social and legal environment are key components to their propensity to develop an organic cyber capability. In addition, leadership buy-in can shape whether cyber emerges as a well-resourced capability that is embraced by military or intelligence organizations as a means of achieving geopolitical aims.

Grand Cyber Arms Bazaar: A Framework for Categorizing Sophistication

One challenge that government and private sector executives will face with the evolving cyber threat landscape is how to posture their organization to minimize surprise around the emergence of new cyber actors and effects. A growing number of nefarious actors are acquiring capabilities from commercial sources, cyber criminals, and open sources. Some are hiring former intelligence and military officers who have cyber expertise. Others are establishing professional cadres to develop, maintain, and use indigenous capabilities. This expanding array of actors increasingly

[5] Bing, Christopher and Joel Schectman (2019, January 30). Reuters. *Project Raven: Inside the UAE's Secret Hacking Team of American Mercenaries*. Retrieved from: https://www.reuters.com/investigates/special-report/usa-spying-raven/

recognize cyber as an asymmetric capability that can be employed below the threshold of armed conflict to signal displeasure with established powers or otherwise deter them.

- This section presents a framework, a "grand cyber arms bazaar," to help distinguish among a growing range of actors, all having access to advanced capabilities, based on their organizational maturity (advanced, emerging, or opportunistic) and operational intent (collection, profit, or disruption).

- We begin by orienting the reader to the framework at a high level. We then delve into greater detail on two distinguishing factors among threat actors: organizational maturity and operational intent. The next section offers three examples of applying the framework.

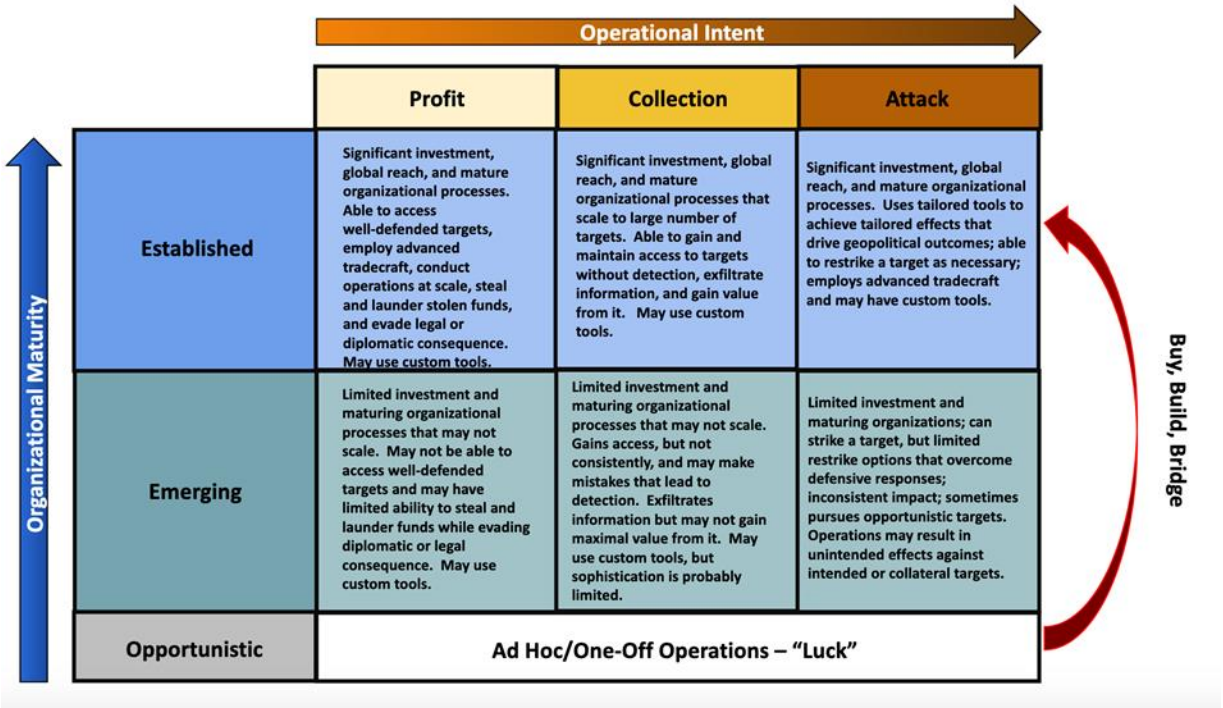
Strolling the Grand Bazaar

Our framework is presented in Figure 1 below. The idea of a "grand bazaar" is motivated by the range of cyber tools that are available to the full range of state and non-state threat actors. Nonetheless, these actors likely will achieve varying degrees of success in the cyber realm, despite having access to comparable capabilities. One influencing factor is their ability to "professionalize" cyber capabilities in mature organizations that integrate a mix of technical, operational, and other skills and develop repeatable processes for conducting cyber operations. Another factor is operational intent, which spans a range from simple "smash and grab" collection (theft), to complex operations calibrated to achieve precise and reliable disruptive effects.

- We identify three categories of actors based on increasing levels of organizational maturity: opportunistic, emerging, and established. A few factors can enable actors to quickly "leapfrog" between categories. For example, actors may buy capabilities and talent or develop partnerships that allow them to tap into external capabilities. Leadership emphasis can also drive rapid maturation by directing resources and talent to cyber over other priorities.

- Intent can range from profit to collection to attack. In some cases, it may be possible to draw complexity distinctions among these motives. For example, conducting a cyberattack that achieves reliable and repeatable impact on a critical infrastructure or other target may require an understanding of how that target operates and countering defenders' efforts to reconstitute. Nonetheless, we acknowledge that mature organizational processes provide a foundation for actors to mount highly sophisticated operations aimed at profit or theft.

Figure 1: The Grand Cyber Arms Bazaar Framework



Organizational Maturity

Established Actors: Those with the most advanced, accurate, and agile tools are considered "established" actors. In-house developed tools with wide availability and customization are developed to gain and maintain access to their targets, including those that are well defended. Established actors have extensive resources, including time and money to achieve persistence, and are capable of achieving global reach using advanced tradecraft. They have products, process, and people aligned to them, as well as robust risk management programs to consider and mitigate the effects of exposure. Nation-states who fall in this category have the ability to leverage sophisticated tools to target other nation-states with the intent of driving geopolitical outcomes. Established actors leverage tools like malware, such as Zebocry, to target diplomats, defense officials, and ministry of foreign affairs staff with the aim of stealing login credentials, keystrokes, communications, and sensitive files.[6] When these tools are deployed in coordination with military efforts, the scale of impact is markedly wider.[7]

[6] GReAT (2019, August 1). *APT trends report Q2 2019*. Retrieved from: https://securelist.com/apt-trends-report-q2-2019/91897/

[7] For example, the Russian-backed group Sandworm used a destructive piece of malware called NotPetya to attack Ukraine and through a widely used tax software. Although targeting was regional, NotPetya inadvertently spread on

Emerging Actors: Emerging actors include nation-states, criminal organizations, and others who have defined processes, capabilities, and a history of targeted operations. However, there is a clear hallmark of emergent actors: their attempts are not consistently successful to the extent of established actors. They are able to expend resources to strike a target but have no immediate restrike capabilities. While attacks are occasionally successful, impacts are inconsistent. Further, while these actors have some tradecraft, it is limited. These groups have the beginning of organizational maturity, and are on the cusp of developing the products, processes, and people necessary to contend with the "established" actors. Some of these actors are less technology-capable than the established actors, but look to global powers such as China and Russia for ideas. These ideas and resources provided by established powers could lead a low-level actor to become an emerging threat.[8] Regardless of whether these nations are buying, building, or bridging their capabilities, they remain a threat to be tracked, especially as their geopolitical interests incentivize the use of cyber weapons.

Opportunistic Actors: Generally, opportunistic actors are associated with low-level cybercriminal activity. The markets in which they operate are dispersed, diverse, and segmented; they are constantly innovating to keep pace with current trends and avoid law enforcement intervention.[9] Further, they typically have a small bench size, do not utilize large-scale processes, and are acting for financial gain or to achieve notoriety. These are actors whose methods are not repeatable and tend to be in the "right place at the right time" which is what leads to their success. Although often leveraging open source tools or existing code, some cybercriminals are now reported to be using tools that are more sophisticated and techniques developed and leaked by other actors.[10] In the opportunistic category, there are a vast number of entities, organizations, and nation-states with these capabilities, especially as compared with emerging and established actors.

Another method to distinguish emerging and established actors, particularly, is the level of offensive cyber capability. One academic interviewed made a further distinction in offensive cyber capabilities by distinguishing between levels of attack precision, with high precision attacks typically associated with nation-states attempting to achieve a specific effect against a specific target with minimal to no collateral damage. Low precision attacks, which are less complicated and less costly, are normally associated with no specific target or time frame and unconstrained by

---

a global scale, crippling international corporations such as Maersk and Merck as well as shipping, construction, and agriculture industries.

[8] Sherman, Justin (2019, July 25). *Digital authoritarianism and the threat to global democracy*. Retrieved from: https://thebulletin.org/2019/07/digital-authoritarianism-and-the-threat-to-global-democracy/

[9] United States. Cong. House. Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance. *Hearing on Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. Mar. 15, 2018.* Washington: GPO, 2018. (statement of Lillian Ablon, the RAND Corporation).

[10] Department of Defense, Defense Science Board. 2013. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. Washington, DC: The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

collateral damage. Another researcher differentiated offensive cyber capabilities by three components:

- People: operators, developers, system administrators, front office personnel, strategic and legal experts, etc.
- Exploits and tools: their origination and usage
- Infrastructure: degree of outsourcing of cyber infrastructure

Figure 2: Example of the Grand Cyber Arms Bazaar Framework

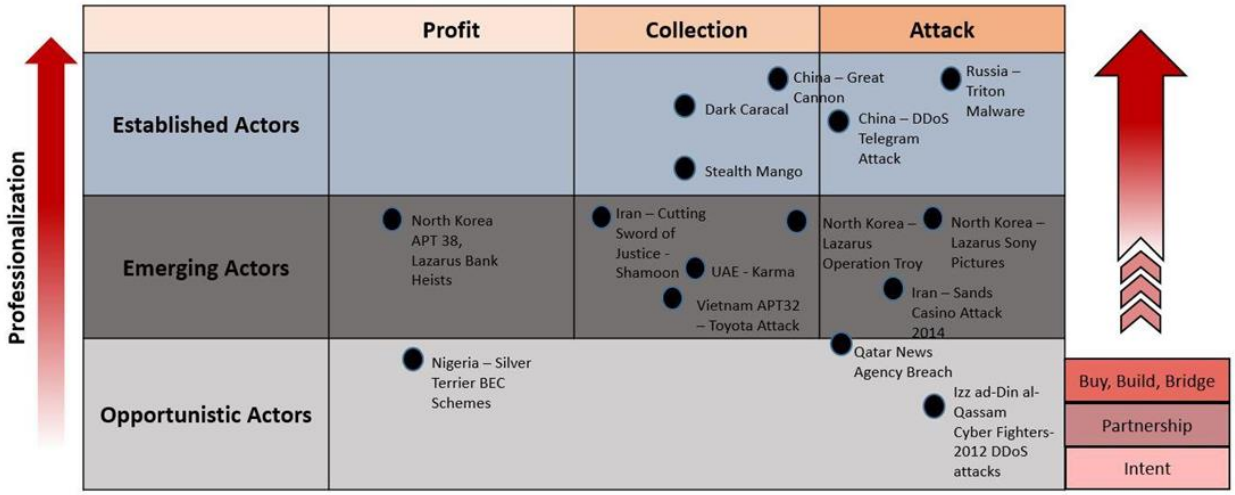


Figure 3: SilverTerrier and Iran

Silver Terrier

Silver Terrier is a Nigerian cybercriminal group known for their business email compromise schemes. One expert considered Nigeria could be the "next" country to rise through the ranks of dangerous or threatening cyber actors. However, examining not only the tools but the motive of their activity, it is clear that Silver Terrier's current plans do not include driving any geopolitical outcomes (see Figure 2).

Iran

In the early 2000s, many considered Iran to be a lower-tier actor; however, the nation has made drastic improvements in their capabilities, to the surprise of many US military leaders. Iran

views cyber weapons as party of the asymmetric military capabilities it can use against countries like the United States, which feeds its intent to continue to rise as an "established" actor.

Operational Intent

One of the most important differentiators among these actors is their motivation. Intentions widely vary for cyber operations but can nevertheless elevate their status between tiers. Examples of intent include financial gain, power or the advancement of political agendas, or geopolitical outcomes (see the "emerging" and "established" categories in Figure 1). Many experts emphasized that it is futile to observe what capabilities actors possess in a vacuum. One of the most important factors in a nation-state's propensity to be a threat is their intent, and subsequently their willingness to deploy their capabilities.

Financial Gain: Nation-state cyber campaigns tend to be carried out in pursuit of surveillance, espionage, and targeting of adversary critical infrastructure. However, there is another motivator that impacts governments, corporations and individuals alike: profit. Many governments and institutions, particularly financial institutions, have extensive stores of sensitive information which can be easily liquidated for financial gain if a cyber actor is successful. Adversaries leverage crimeware, known vulnerabilities, phishing, spear phishing, and smash-and-grab techniques to attain financial gain at the expense of their target.[11] Actors within this category range from ad-hoc cyber criminals to nation-states whose motivations and hostilities are exacerbated by income loss and international effects of economic sanctions.[12]

Collection & Surveillance: Beyond using cyber weapons to conduct profit-driven outcomes, threat actors conduct operations with the intent of data collection, surveillance, and espionage. They employ information without the consent or knowledge of their intended target. Actors use these tools to target individuals, groups, industries, or even other nation-states. Collection techniques are also prevalent in regional conflicts, for example, the United Arab Emirates (UAE) has used collection tools such as Karma for a campaign that monitored targets including the Emir of Qatar, Turkish national leadership, and a human-rights activist in Yemen.[13]

---

[11] United States. Cong. House. Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance. *Hearing on Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. Mar. 15, 2018.* Washington: GPO, 2018. (statement of Lillian Ablon, the RAND Corporation).

[12] Halpern, Sue (2019, July 18). New Yorker. *How Cyber Weapons Are Changing the Landscape of Modern Warfare*. Retrieved from: https://newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

[13] Schectman, Joel and Christopher Bing (2019, January 30th). Reuters. *Exclusive: UAE Used Cyber Super-Weapon To Spy on iPhones Of Foes*. Retrieved from: https://www.reuters.com/article/us-usa-spying-karma-exclusive/exclusive-uae-used-cyber-super-weapon-to-spy-on-iphones-of-foes-idUSKCN1PO1AN

Activity associated with the Dark Caracal group highlights how cyber capabilities can offer global reach to new cyber actors. Development of collection-driven tools, uncovered by cybersecurity firm Lookout Mobile in partnership with the Electronic Frontier Foundation (EFF), has been linked to the Lebanese government, specifically to the Beirut headquarters of the Lebanese General Directorate of General Security. As described in a report from Lookout Mobile and the EFF, this activity has targeted governments, militaries, various industries, financial institutions, and defense contractors. Data uncovered by Lookout Mobile showed documents, call records, audio recordings, secure messaging content, contact information, text messages, photos and account data that had been collected by the Dark Caracal actors.[14]

Many, including United Nations Special Rapporteur David Kaye, have raised concerns over the availability of these collection-based tools. Various technologies can be purchased and leveraged by nation-states and used in human rights violations that lead to detention, tortures, and extrajudicial killings.[15] The reality of collection efforts spans far beyond simply the monitoring of a person or group's private information and location—it manifests itself in grievous human rights violations and, in many cases, loss of life.

Offensive Attack: Cyberattacks can occur for a variety of reasons, but their overall motive is generally to inflict damage to their targets. Actors deploy malicious methods to invade, manipulate and execute missions on the intended target. One such prevalent method is the distributed Denial-of-Service (DDoS) attack. Adversaries typically conduct DDoS attacks for political purposes and to support other malicious activities such as distraction, hacktivism, and extortion. Since March of 2019, DDoS attacks have targeted computer systems controlling the power supply in Los Angeles and Salt Lake City; the Central Bank; Ministry of Foreign Affairs; and the Presidential Office of Ecuador, as well as the messaging application Telegram, which China used to investigate demonstrations in Hong Kong.

Nation-states often use offensive attacks to hack and attack the networks of other nation-states and adversaries. For example, the Russian military in June 2017 launched the NotPetya cyberattack against Ukrainian networks. This software, "which quickly spread worldwide, causes billions of dollars in damage across Europe, Asia, and the Americas" and was part of a Russian effort to destabilize Ukraine, according to a White House statement in February 2018. Attacks can have a variety of targets, from governments to private companies. For example, Iranian cyber actors in February 2014 targeted Sands Las Vegas Corporation, according to public statements in early 2015 by then US Director of National Intelligence James Clapper. The attack may have been motivated

[14] Lookout. 2012. *Dark Caracal, Cyber-espionage at a Global Scale*. USA: Electronic Frontier Foundation. Retrieved from: https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

[15] Anstis, Siena, Ron Deibert, Miles Kenyon, and John Scott-Railton. Citizen Lab. *The Dangerous Effects of Unregulated Commercial Spyware*. Retrieved from The Citizen Lab: https://citizenlab.ca/2019/06/the-dangerous-effects-of-unregulated-commercial-spyware/

by public comments by the casino's owner, which may have drawn the ire of Iranian officials. Cyberattacks such as NotPetya and the Sands incident currently are being performed at the hands of advanced and established cyber actors, however, experts fear the ability of emerging or even opportunistic actors to buy, build, and bridge these capabilities.

Applying the Framework: Case Studies

Case Study #1: North Korea

We identify North Korea as an "emerging" actor overall, but they could fall in the "established" category for cyber crime. During the past decade, the North Korean government has sponsored cyber operations of increasing sophistication aimed at financial gain for the regime and intelligence collection. They have also used cyberattack as a means of signaling displeasure for perceived slights to the regime. Across this range of motives, the North Koreans have shown a higher risk tolerance for aggressive cyber activity compared to other emerging actors.

Financially Motivated Activities

The North Korean regime has used cyber means to acquire funds to avoid international sanctions since at least 2015. The vast sums stolen in multiple operations spanning years suggests this country may fall in the "established" category in our framework, at least in the area of cyber crime. Their success likely stems in part from adroit exploitation of technological trends by North Korean cyber actors who have taken advantage of security weaknesses in financial institutions, the difficulty of tracing cryptocurrencies, and global money laundering networks.

- North Korea has used cyber operations to steal as much as $2 billion to generate income and sidestep United Nations (UN)-imposed sanctions, according to press reports in early August 2019 that detailed a still-unpublished UN report.[16] The UN experts reportedly were investigating , "at least 35 reported instances of DPRK actors attacking financial institutions, cryptocurrency exchanges, and mining activity designed to ear foreign currency" in some 17 countries, according to the same press report.

- A criminal complaint lodged in June 2018 by the US Department of Justice (DOJ) against North Korean actor Park Jin Hyok describes a "wide-ranging, multi-year conspiracy to conduct computer intrusions and commit wire fraud by co-conspirators" working on behalf of North Korea.[17] The complaint implicates these conspirators in the fraudulent

[16] BBC. North Korea stole $2bn for weapons via cyber-attacks (2019, August 7). Retrieved from: https://www.bbc.com/news/world-asia-49259302

[17] United States District Court for the Central District of California (2018, June 8). Criminal Complaint: *United States of America v. Park Jin Hyok, Defendant*. Retrieved from: https://www.justice.ggov/opa/press-release/file/1092091/download

transfer in February 2016 of $81 million from the Bangladesh Bank and in computer intrusions and cyber heists having attempted losses of over $1 billion from 2015 to 2018.

- A South Korean intelligence agency in early 2018 reportedly informed South Korea's National Assembly of North Korean involvement in the heist in January 2018 of $526 million from Japanese cryptocurrency exchange Coincheck.[18] South Korean intelligence further alleged that North Korean actors had stolen on the order of tens of millions of dollars from South Korean cryptocurrency exchange providers.

Despite North Korea's success with cyber-enabled theft, the global Wannacry malware outbreak in May 2017 highlights the potential dangers of unintended consequences from cyber operations employing virulent software exploits. This outbreak, attributed to North Korea in late 2017 by then Homeland Security Advisor Tom Bossert, impacted hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries, according to a White House press statement.[19]

One driver for the malware's rapid spread was its use of the EternalBlue, an exploit attributed to NSA which an unidentified group known as the Shadow Brokers publicized in April 2017.[20] The North Korean actors may have underestimated their ability to control this virulent exploit, despite incorporating a "kill switch" in the Wannacry code.

Collection-Driven Activities

However, beyond simply profit-driven motives, North Korea has been active in the "collection" arena as well. For example, Lazarus Group, a threat group attributed to the North Korean government, deployed Operation Troy in 2009. Operation Troy was a campaign that aimed to spy on and disrupt South Korea's military and government activities. Lazarus Group carried out their operations using multiple types of malware, which allowed remote access to the targets' environments.[21]

---

[18] Nikkei Asian Review (2018, February 6). North Korea Suspected in Coincheck. Retrieved from: https://asia.nikkei.com/Spotlight/Bitcoin-evolution/North-Korea-suspected-in-Coincheck

[19] Brady, James S. (2017, December 19). *White House Press Briefing. Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*. Retrieved from: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917

[20] McNeil, Adam (2018, February 8). MalwareBytes Labs. *How Did the WannaCry Ransomworm Spread?* Retrieved from: https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread

[21] Sherstobitoff, Ryan and Itai Liba, James Walter (2018). McAfee. *Dissecting Operation Troy: Cyber Espionage in South Korea. Santa Clara, CA: McAfee.* Retrieved from: https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf

Attack-Driven Activities

Many remember the 2014 Lazarus-led Operation Blockbuster, better known as the Sony Pictures Entertainment Attack. Acting under the name "Guardians of Peace," North Korean government actors targeted Sony Pictures Entertainment (SPE) networks, employees and their families, as well as proprietary corporate information. Once inside SPE's network, the actors stole (and leaked) movies and other confidential information and effectively rendered thousands of computers inoperable, according to a DOJ indictment.[22] Along with this attack, the group threatened the company against the release of a film that they considered slanderous to the North Korean regime.

The SPE attack illustrates the potential for a regional power to exploit today's interconnected environment to cause effects within US borders that would not have been possibly previously. The incident also shows the potential for other actors to adopt similar tactics to signal displeasure for US actions, including by the private sector, using means considered short of war.

North Korea's ability to achieve a finite aim demonstrates an "emerging" level of cyberattack capability. However, it does not show the ability to repeatedly and reliably use cyberattack to achieve clear geopolitical aims, which would be characteristic of an "established" actor in the attack realm.

Drivers

Experts claim that North Korea currently lacks some of the definitional characteristics of an established cyber power; however, several drivers could propel them to the level of an established power over time. North Korea leverages China for elevating its capability through training, and even draws lessons from Chinese military doctrine.[23] Aside from political and economic ties to China, North Korea has been reported to train their most promising hackers in Shenyang, a one-hour train ride from the North Korean border.[24] As discussed, North Korea is rife with cyber intent from avoiding sanctions to making a geopolitical impact on their enemies. Additional drivers include their "bridging" of capabilities through utilization of advanced cyber criminal networks worldwide.

---

[22] United States District Court for the Central District of California (2018, June 8). *Criminal Complaint: United States of America v. Park Jin Hyok, Defendant.* Retrieved from: https://www.justice.ggov/opa/press-release/file/1092091/download

[23] Kong, Ji Young, Jong In Lim, Kyoung Gon Kim (2019). 2019 International Conference on Cyber Conflict: Silent Battle. *The All-Purpose Sword: North Korea's Cyber Operations and Strategies*. Retrieved from: https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf

[24] Tribune News Service (2018, February 1). *How did barely connected North Korea become a hacking superpower?* Retrieved from: https://www.scmp.com/print/news/world/article/2131470/north-korea-barely-wired-so-how-did-it-become-global-hacking-power

Case Study #2: Vietnam

Since at least 2012, threat actors allegedly linked to the Vietnamese government have conducted increasingly sophisticated and persistent campaigns targeting various sectors. The activity of Vietnamese-sponsored threat actors, combined with their government signaling increasing investment in cyber capabilities, indicates that Vietnam is an emerging player in cyberspace. Although they are not in the established tier, Vietnam exhibits key drivers, including monetary and personnel investment, as well as leveraging off-the-shelf tools and informal partnerships that will allow the country to rapidly push its cyber power forward across the board.

Collection-Driven Activities

The most prominent actor for Vietnam-based cyber activity is the OceanLotus Group, also known as APT32. This activity was first detected in 2012, when it was observed targeting intellectual property and confidential business information from organizations in China, Vietnam, and the Philippines.[25] The group has persisted since it came onto the scene, also targeting human rights organizations, research institutes, and journalists.[26] Additionally, OceanLotus has deployed numerous custom-built tools in its operations and at times has persisted on networks for more than a year, highlighting there is likely sizeable investment in the group.[27] APT32 represents the most notable example of a threat actor not sponsored by China, Iran, Russia, or North Korea - conducting significant activity in support of, and likely sponsored by, a foreign government.[28]

- This activity provides a canonical example of an emerging collection actor. As more actors gain access to increasingly sophisticated capabilities through various means, it is likely that similar patterns of cyber activity sponsored by other governments will be detected.

Attack-Driven Activities

In early 2018, Vietnam announced the creation of the "Cyberspace Operations Command," elevating cyber to a top-tier priority.[29] The stated intent of the 10,000-strong unit is to "counter

---

[25] Hay Newman, Lily (2017, May 24). Wired. *An Up-Close View of the Notorious APT32 Hacking Group in Action*. Retrieved from: https://www.wired.com/2017/05/close-look-notorious-apt32-hacking-group-action/

[26] CFR. *Cyber Operations Tracker: Ocean* Lotus. Retrieved from: https://www.cfr.org/interactive/cyber-operations/ocean-lotus

[27] Dahan, Assaf (2017, May 24). Cybereason. *Operation Cobalt Kitty: A Large-Scale Apt In Asia Carried Out By The Oceanlotus Group.* Retrieved from: https://www.cybereason.com/blog/operation-cobalt-kitty-apt

[28] Carr, Nich (2017, May 14). FireEye. *Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations*. Retrieved from: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

[29] Parameswaran, Prashanth (2018, January 12). The Diplomat. *What's Behind Vietnam's New Military Cyber Command?* Retrieved from: https://thediplomat.com/2018/01/whats-behind-vietnams-new-military-cyber-command/

'wrong' views on the Internet." This development, combined with Vietnam's strong collection capabilities, could lay an organizational and technical foundation for creating a cyberattack capability should future regional dynamics in South East Asia warrant.[30]

- Press reports from mid-2017 linking APT32 to the public disclosure of sensitive Philippine government documents, including the transcript of a call between Philippine President Rodrigo Duterte and the US President, suggest that Vietnam may have begun to apply its cyber collection capabilities to hack-and-leak operations aimed at embarrassing a regional regime.[31] This tactic may arise in the future as a first foray by other emerging cyber actors into offensive cyber operations that seek effects beyond collection and surveillance.

Financially-Motivated Activities

Another factor in the mix is the rise of Vietnamese cybercriminal actors, reportedly an intended target of the country's controversial cyber law.[32] While there are not any reported occurrences of Vietnam coopting cybercriminals within its borders to achieve the goals of the state, this trend has been a common way for other nation-states to enhance capabilities and expand its attack surface. A recently shuttered Vietnamese hacking website had a membership of more than 14,000 before it was shut down, highlighting the growing cyber talent within the country whose threat actors are also allegedly involved in globally well-known underground forums.[33]

Drivers

Vietnam is committed to aggressive economic growth and enhancing the competitiveness of its domestic industries; the operation of APT32 to date point to the government's willingness to engage in cyber operations to achieve those goals. Vietnamese officials have echoed the idea that cyberspace is critical for the security and development of the country.[34]

---

[30] Nguyen, Mi (2017, December 26). Reuters. *Vietnam unveils 10,000-strong cyber unit to combat 'wrong views'* Retrieved from: https://www.reuters.com/article/us-vietnam-security-cyber/vietnam-unveils-10000-strong-cyber-unit-to-combat-wrong-views-idUSKBN1EK0XN

[31] Bing, Chris (2017, May 31). CyberScoop. *A Stolen Trump-Dutere Transcript Appears to be just One Part of a Larger Hacking Story*. Retrieved from: https://www.cyberscoop.com/apt-32/trump-duterte-hacking-xi-jinping-vietnam

[32] Lindsey, Nicole (2019, January 14). CPO Magazine. *Vietnam's Controversial New Cyber Law Could Entangle Google and Facebook in a Battle Over Freedom of Speech*. Retrieved from: https://www.cpomagazine.com/cyber-security/vietnams-controversial-new-cyber-law-could-entangle-google-and-facebook-in-a-battle-over-freedom-of-speech/

[33] Vijayan, Jay (2019, June 5). Dark Reading. *Vietnam Rises as Cyberthreat*. Retrieved from: https://www.darkreading.com/attacks-breaches/vietnam-rises-as-cyberthreat-/d/d-id/1334890

[34] Parameswaran, Prashanth (2018, January 12). The Diplomat. *What's Behind Vietnam's New Military Cyber Command?* Retrieved from: https://thediplomat.com/2018/01/whats-behind-vietnams-new-military-cyber-command/

Case Study #3: Artem Radchenko and Oleksander Ieremenko

A 16-count indictment unsealed in January 2019 charged Ukrainian nationals Artem Radchenko and Oleksander Ieremenko with securities fraud conspiracy, wire fraud, and computer fraud, according to a public release from the US DOJ.[35] The indictment alleges that these individuals hacked into the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system operated by the US Securities and Exchange Commission in order to steal thousands of files including annual and quarterly earnings reports containing confidential, non-public, financial information, which publicly traded companies disclose to the SEC. This activity allegedly occurred from February 2016 through March 2017. Radchenko and Ieremenko allegedly used a series of targeted cyberattacks, including directory traversal, phishing, and infecting computers with malware. The indictment further alleges that Radchenko recruited to scheme traders who were provided with stolen test filings, which often contain information similar to corporations' final filings, so they could profit by trading on the information before the investment went public.

- This activity fits the profile of an emerging, profit-driven non-state cyber actor. Radchenko and Ieremenko identified and used cyber means to target a high-profile SEC database containing sensitive corporate earnings information. They successfully exfiltrated data over an extended time period and worked with recruited traders to use the stolen information for profit. However, these actors prior to their indictment did not demonstrate an ability to scale their operation to illicitly obtain vast sums comparable to other cyber crime actors, such as those tied to the North Korean government.

Policy Challenges: Deterrence, Redlines, and Escalation

The lack of rules and consequences within the cyber realm has resulted in several policy challenges, namely, a *de facto* tolerance of cyber operations that fall below a clear threshold of war. This tacit acceptance creates inertia for moving towards a consensus - and is driven by immature approaches to deterring cyber activity and a lack of international consensus on norms to guide nation-state behavior in cyberspace, including clear redlines for when cyber effects become an act of war. The current climate is one in which cyber activity that crosses an unclear threshold or causes unintended consequences could escalate into armed conflict. Furthermore, an absence of established norms to guide nation-state and non-state actors' behavior exacerbates confusion over the status of private sector companies, and how commercial entities that offer cyber services and capabilities should operate. This section addresses the challenges of deterrence, norms and redlines, and escalation.

[35] United States. Department of Justice, Office of Public Affairs (2018, January 15). *Two Ukrainian Nationals Indicted in Computer Hacking and Securities Fraud Scheme Targeting U.S. Securities and Exchange Commission.* Retrieved from: https://www.justice.gov/opa/pr/two-ukrainian-nationals-indicted-computer-hacking-and-securities-fraud-scheme-targeting-us

Dearth of Effective Approaches to Deterrence

While it can be argued that Western deterrence and policies in a traditional sense have led to a state of relative peace since 1945, this same policy-driven leadership has not been present when it comes to the use and regulation of cyber capabilities. Western governments have not been consistent in their response to hold actors accountable for cyber incidents.[36] This is in part due to the diverse set of actors in cyberspace, the creation of policy reactively, and the difficulty of attribution when it comes to cyberattacks.

Non-state actors represent a unique challenge to deterrence because they are often not susceptible to diplomatic or military suasion in the same manner as nation-states. Several government officials advised that the problem with holding non-state actors accountable is that retaliatory actions and policy standards such as sanctions and treaties are not applicable, because they are not government entities and typically do not have the same concern about the opinions of the international community. These groups also often lack clear territory or physical locations that can be targeted by military means, or they may reside in countries that tolerate such activity where the use of military force would not be feasible for other reasons.

In the past, the US (DoD in particular) has acknowledged there is an issue with cybersecurity policy and has outlined strategies going forward. However, there remains a lack of effective policy development, response to incidences, and metrics to determine progress.[37] Further, US decision-making and policy has been reactive rather than proactive, and driven by specific events such as distributed denial of service (DDoS) attacks against the US financial sector between late 2011 and mid-2013, which led to the indictment in early 2016 of seven Iranian actors employed by two firms that had performed work on behalf of the Iranian government, including the Islamic Revolutionary Guard Corps.[38] Those attacks caused hundreds of thousands of customers to be unable to access their accounts and resulted in companies losing tens of millions of dollars in remediation costs. Incidences such as these have led the United States to indict and publicly attribute the activity of nation-state actors as part of attempts to dissuade these actions.[39,40,41] The efficacy of this kind of

---

[36] Department of Defense, Defense Science Board. 2013 . *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. Washington, DC: The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

[37] ibid.

[38] United States. Department of Justice, Office of Public Affairs (2016, March 24). *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*. Retrieved from: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

[39] ibid.

[40] United States District Court for the District of Columbia (2018, February 16). Indictment. *United States of America v. Internet Research Agency LLC A/K/A Mediasintex LLC, etc., Defendants.* Retrieved from: https://www.justice.gov/opa/press-release/file/1035562/download

[41] ibid.

policy is debatable, and its creation does not place the US at the forefront of developing international cyber policy that will shape the future; rather, it creates policy that correlates to historical incidents.[42] There is also hesitation with enacting effective policy and response because of the difficulty in attributing or possibly misattributing cyber activity. The United States' history of reactive cyber policies and failure to enact clear and consistent responses has helped facilitate a *de facto* norm for acceptance of certain types of offensive cyber activity by foreign threat actors.

Lack of Redlines

The lack of clear international norms regarding the use of cyber capabilities has led to the creation of unwritten rules among cyber actors on how to operate.[43] The default "red line" that has been drawn among nation-states is defined by the use of cyber capabilities with consequences that lead to war, and anything below that line being acceptable. The problem with this redline is that there is no consistency on what the range of cyber behavior should be below this threshold. Several experts mentioned that countries such as China, Russia, Iran, and North Korea all seem to be more tolerant of operational and diplomatic risk than the West. The imprecision of the redline becomes more of an issue when considering non-state actors who have little regard for law that is clearly written.

- One aspect of this environment is the lack of clear norms related to cyber operations against private sector companies.[44] Some foreign actors pursue this tactic as a means of applying pressure on the US short of war to change its policies or to drive an ideological agenda.

- The emergence of private sector firms and criminal groups that are willing to sell cyber capabilities has made this environment more tenuous,[45,46] as there are also no agreed upon international regulations guiding what types of capabilities are acceptable to create and sell.

---

[42] Pomerleau, Mark (2019, February 21). Fifth Domain. *New Report Questions Effectiveness of Cyber Indictments*. Retrieved from: https://www.fifthdomain.com/industry/2019/02/21/new-report-questions-effectiveness-of-cyber-indictments/

[43] Ranger, Steve (2018, December 4). ZDNet. *What is cyberwar? Everything you need to know about the frightening future of digital conflict*. Retrieved from: https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

[44] Ranger, Steve (2014, April 24). TechRepublic. *Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyber War*. Retrieved from: https://www.techrepublic.com/article/inside-the-secret-digital-arms-race/

[45] Stockton, Paul and Michele Golabek-Goldman (2013). Yale Law & Policy Review, Volume 32, Issue 1, Article 11. *Curbing the Market for Cyber Weapons*. Retrieved from: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1660&context=ylpr

[46] Zilber, Neri (2018, August 31). *The Rise of Cyber Mercinaries*. Retrieved from: https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/

Although there has been dialogue about creating rules for cyber conflict and operations, such as the Tallinn Manual, Tallinn Manual 2.0,[47] and Digital Geneva Convention proposed by Microsoft,[48] there is still no agreement across the international community. An academic noted that the redline has been continually moving towards more destructive behavior,[49] with incidents such as Stuxnet, WannaCry, and NotPetya, which leads to the potential for escalation and unintended consequences.

Escalation and Unintended Consequences

As cyber effects move increasingly closer to what are universally viewed as acts of war, there is the increasing potential to cross a redline that elicits kinetic or military response. The lack of agreed-upon redlines in this area introduces a risk of miscalculation among nations, particularly in crisis situations. Governments may operate under differing perceptions that may or may not be evident to their rivals. A cyberattack occurring during a period of inflamed tensions could unintentionally place a government in a situation in which it would have to respond to assuage popular anger or maintain credibility in other diplomatic or military arenas. The possibility of a cyber operation causing unintended consequences adds further risk.

- One academic noted that in some cases cyberattack may be perceived as a non-escalatory tactic that could be used when kinetic means may not be desirable, but cautioned that cyber has not yet been escalatory. In this vein, the academic offered the example of the US drone shot down in June 2019 by Iran's Islamic Revolutionary Guard Corps. The expert explained that this incident likely involved some calculus by the government of Iran; shooting down the drone would send a message without the provocative impact of causing US casualties. The expert, noting press reports of an alleged US cyber response, suggested that this tactic offered an "escalation-controlled" response because no Iranians would die. However, the expert cautioned that the alleged cyber response could risk unintended consequences or a "tit-for-tat" cyber dynamic, both of which could have escalatory consequences.

- An actor not governed by rules could underestimate the potential destruction a cyber capability has, overestimate their ability to maintain control of a capability, or simply act

[47] NATO Cooperative Cyber Defence. *Tallinn Manual 2.0*. Retrieved from: https://ccdcoe.org/research/tallinn-manual/

[48] Guay, Joseph and Lisa Rudnick (2017, June 25). UNHCR Innovation Service. *What the Digital Geneva Convention Means for the Future of Humanitarian Action.* Retrieved from: https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

[49] Gertz, Bill (2017, November 16). Free Beacon. *NSA: Cyber Attacks Are Becoming More Sophisticated, Aggressive, and Disruptive*. Retrieved from: https://freebeacon.com/national-security/nsa-cyber-attacks-becoming-sophisticated-aggressive-disruptive/

recklessly. This was observed in NotPetya and Stuxnet, where these capabilities propagated beyond their initial intended victims.

A Few Futures to Consider

We describe two alternative futures that represent potential boundary cases for geopolitical impacts resulting from the global diffusion of cyber capabilities in what amounts to a "grand cyber arms bazaar." In one extreme, the complexity and volatility of this dynamic, as described in previous sections, results in a rapid escalation of tensions between actors that has the potential of crossing the threshold of armed conflict. In the other scenario, the global community reaches a diplomatic, technological, or other inflection point that changes the current dynamic of rapid diffusion of capabilities applied by an increasing number of actors without clear norms or restraints.

Scenario A: Rapid Escalation

This scenario walks through how a combination of factors, both cyber and non-cyber, could collectively lead to an escalation of tensions between two nations, potentially leading to kinetic action. We assume the current trends of wide availability of cyber tools, an increasing number of actors, and lack of norms or other restraints continue unabated. In this environment, foreign actors take increasingly risky actions with little regard for repercussions, or their cyber capabilities cause unintended collateral effects. Technology also continues its rapid advance, with increasingly interconnected technologies being incorporated into critical infrastructures and virtually every aspect of everyday life. This increases the chances of a cyber event causing physical harm that crosses a kinetic response threshold. Attribution of cyber activity also remains challenging and some governments employ non-state actors to "jump start" their capabilities or operate with plausible deniability.

In the West, interaction between the government and private sectors has not evolved to meet the threat. Without public-private partnerships that evolve with cyber developments and threats, the ability to mitigate tensions becomes more difficult. Without well-established effective partnerships, governments are slower to respond and keep up with cybersecurity developments or work with the private sector to bring about appropriate regulations and unified information sharing practices. Without the support or mandate from the public sector to set effective cyber policy, companies in the private sector may not be equipped or incentivized to allocate enough of their budget to cybersecurity.

It is not difficult to visualize a situation where in an already fragile environment, one miscalculated attack can spark a series of responses that could include steps nearing a physical attack. In this instance, a state actor known as Country X has temporarily employed the cyber capabilities of a domestic criminal organization. This criminal organization has been testing out adversarial artificial intelligence (AI) on vehicles and successfully altered some of the vehicle's systems.

Country X is developing its own capabilities but uses non-state actors as it builds its own arsenal and tests out new tactics under the guise of the criminal organization. While it hopes to develop skills to launch sophisticated, targeted attacks on power-grids or financial systems should the need and opportunity arise, Country X first assesses and learns from the capabilities of the criminal organization. It directs the criminal organization to continue conducting progressively more sophisticated attacks on its behalf. While some attacks are discovered, none result in significant responses.

A controversial global event could motivate the criminal organization to set off a series of simultaneous cyberattacks using their adversarial AI that result in significant financial losses, sensitive data leaks, and/or the fear of possible destruction of life and property. Whether these effects were intended and whether the criminals were acting at the behest of Country X remain unclear. To make it worse, the criminals access and release massive volumes of personally identifiable information (PII) and a host of sensitive documents from more than 20 countries. The effects of this incident are particularly severe in Country Y, which is a regional rival of Country X.

While not taking a toll on human life, the overly aggressive cyberattack was unexpected in its range of impact. Suspicions immediately arise regarding Country X's culpability. However, there are no defined parameters or norms to determine how to respond to an unattributed or potentially misattributed attack. The criteria under which a cyberattack crosses a threshold for kinetic response have not been universally agreed upon, although attacks on financial systems and institutions, nuclear systems, and disruption of defense activities are likely agreed upon actions that prompt war.[50]

As noted, Country Y, a regional rival of Country X, was significantly impacted by the incident. Tensions have been simmering for some time over a disputed territory. There have recently been armed clashes, and a Country X-linked insurgent group in the past month conducted a suicide attack in Country Y's capital. The cyber incident further inflames Country Y's population. Protests erupt demanding a response, and Country Y's government is finding it difficult to back down.

Scenario B: Inflection Point

At some point, the trends identified in the previous section reach an inflection point that drives collective action to contain the cyber drivers of geopolitical instability. This might come in the aftermath of an incident that clearly demonstrates the dangers of global cyber diffusion without norms or restraints. Perhaps a cyber event takes an entire nation offline and paralyzes it with no

[50] McDavid, Saundra (2017, July 31). *When Does a Cyber Attack Become an Act of War?* Retrieved from: https://incyberdefense.com/news/cyber-attack-become-act-war/

choice but to seek de-escalation.[51] Such an incident might arise as a cyber analog to the Cuban Missile Crisis of 1962, but likely would not have the same stakes for human existence. The emergence of a new technology could also act as a restraining factor. For example, the integration of AI capabilities could lead to a fundamental shift in the balance between cyber offense and defense that favors the latter.

However it arises, this inflection point has led to cyber norms and the creation of communication channels between governments and the private sector that are designed for use in fast-breaking cyber incidents. Intelligence sharing protocols, to determine attribution for example, are created amongst cooperating organizations. While cyber consultants and advisors have dominated the market for best cybersecurity practices and deterrence services, global institutions begin looking at the macro level legal, privacy, and security implications of cyber advancements and threats.

In this environment, Country X would carefully consider its relationship with the cyber criminal organization. If discovered, the relationship would result in diplomatic or economic consequences designed to outweigh the benefits of having an offensive cyber capability. In addition, this post-inflection environment offers several inducements for Country X to refrain from acquiring destabilizing cyber capabilities.

During a period of tension between Country X and Country Y, the criminal organization based in Country X unleashes a cyber incident with effects comparable to the previous section. As before, this comes in the context of rising tensions with Country Y over disputed territory and a Country X-linked suicide attack in Country Y's capital.

Country Y's government now taps into pre-established communication channels with allied governments as well as Country X. They gain the benefit of timely attribution insights from more technologically advanced countries, which clear the government of Country X. It is determined that the criminal organization's malware went further than intended. Country Y's government wishes to avoid war, and it uses the legitimacy of the international findings as a pathway to de-escalate cyber-driven tensions with Country X.

Conclusion and Recommendations

Over the past decade, we have witnessed the emergence of a "grand cyber arms bazaar." This phenomenon allows a range of nation-states and non-state actors to access tools for financial gain, collection and surveillance, or cyberattack, which will in turn exert an increasing influence on geopolitical, economic, and military balances as an increasing number of actors move from

[51] Morgus, Robert and Justin Sherman (2019, May 17). Just Security. *When To Use the 'Nuclear Option?' Why Knocking Russia Offline Is a Bad Idea*. Retrieved from: https://www.justsecurity.org/64094/when-to-use-the-nuclear-option-why-knocking-russia-offline-is-a-bad-idea/

opportunistic to emerging and established cyber powers. This trend brings a host of implications for executives in the private and public sectors and for the relationship between the public and private sectors in the West.

- Executives in both sectors must posture their organizations for a growing risk of surprise in cyberspace. This trend will be driven by the emergence of new threat actors, the availability of advanced tools, and new vulnerabilities that emerge as technology and interconnectivity advance faster than our ability to control risk and mitigate vulnerability.

- As more actors use cyber effects to advance geopolitical aims, organizations increasingly will need to integrate world events into their network defense processes. Threat intelligence will need to evolve from incorporating indicators of compromise gleaned from detected cyber activity. It will become increasingly important to use geopolitical cues to prioritize finite cyber defense resources, particularly as private sector firms increasingly become front-line targets for foreign actors seeking to shape Western policy short of war. Most firms probably lack mature procedures for doing this.

- Grappling with an increasing risk of surprise will require proactive efforts to increase the operational and technical resilience of organizations. This could include "grease pencil" procedures based on voice and paper communications for operating in the face of sustained degradation to computing and network environments. Technical resilience measures may extend to increased attention to unseen risks in supply chains and third-party vendors and designing computers and networks that incorporate architectural features designed to slow down and contain attackers. Most firms probably have not invested significant effort in these endeavors.

- Government entities, researchers, and think tanks can likely assist public and private sector organizations in posturing for this new environment by developing standards and template processes for using geopolitical analysis to drive cyber defense and maintaining operational resiliency in an increasingly hostile cyber environment.

- Senior executives can prepare their workforces for this environment by developing a consistent and multi-dimensional communications strategy used at all management levels that conveys a sense of urgency in preparing for the new risk environment and identifies high-level priorities and milestones. Senior executives can hold themselves, the management team, and workforce accountable for security and resilience and recognize best practices through bonuses or other rewards. One important undertaking is a deliberate conversation about the appropriate investment in resilience to mitigate a perceived level of future risk.

- New approaches for government and private sector collaboration must be created to ensure national security as private sector firms increasingly become "front line" targets for foreign actors seeking to shape Western policy. Restrictions against the government providing competitive advantage to private firms may need to be updated to reflect this new environment, while still preserving the original intent. Repeatable collaboration processes should define roles and responsibilities of private firms and the various government entities that have a role in protecting national security and conducting law enforcement. These processes must reflect private sector concerns about how information sharing impacts their relationship with regulators. Finally, the clear thresholds should be articulated that help the public and private sectors know when they must come together in the national interest. Most cyber activity will not rise to such threshold.

Appendix 1: Comparison of Concerns and Analytical Challenges Across Industries

Industry	Concern	Analytical Challenge
Financial	Manipulation or hacking of a critical institution (whether an actual exchange or a large financial institution) could have lasting and significant global impacts that could set a state in motion towards a dual cyber and kinetic war.	It is almost certain that hackers are trying to infiltrate financial institutions to steal and sell data. The response a state has to that situation versus a bad actor that wants to use a cyberattack to take down, manipulate, or disrupt the financial system will likely be more severe. Fully understanding the drivers and motivators in this instance is imperative.
Transportation	The role of AI and IoT is increasing, particularly in the transportation industry as mentioned in the scenario above. These technological advancements increase the opportunity for attack and can have physically damaging consequences.	Vulnerabilities are becoming more numerous as a result of more sophisticated software that is lacking equally sophisticated defense mechanisms to protect it.
All	A disruption to the supply chain could have global impacts. Industrial espionage and intellectual property disputes can increase tension between states and contribute to the risk of war.	The risk of an APT is heightened which makes understanding the sophistication of a state and its cyber capabilities important to defend against and also determine attribution. Third parties must meet security standards, otherwise the whole supply chain or significant portions of it are at heightened risk.
Military	The risk of losing personnel can be reduced if a machine, drone, or unmanned weapon can be programmed to conduct an attack. A misjudged cyberattack could have major consequences and/or collateral damage. A lack of defense to protect military resources could also be a game-changer on both sides (the attacker and the attacked).	Programmed/unmanned military equipment utilized in physical warfare could have a significant effect on how a state thinks about war, the rules surrounding war, and the consequences of going to physical war. For less-transparent states or non-states, this will likely increase the risk of miscalculated attacks with greater collateral damage.

Appendix 2: India-Pakistan Case Study

There is substantially less awareness in open-source information regarding the capabilities of India and Pakistan in the offensive cyber dimension, yet some glimpses of what may be underway, combined with educated analysis of potential capabilities, suggests that groups aligned with both are slowly developing a range of more sophisticated capabilities. In 2018, news reports noted that in response to an escalation by Pakistani hackers against India's telecom and national research institutes, the Indian government was establishing a joint agency for cyber warfare.[52] Whether these entities and groups engaged in carrying cyber operations would spill over outside the regional conflict would be one concern – another is the history of proliferation of other military capabilities and whether that may become an issue. A recent example suggests that collateral effects are taking place.

One glimpse behind the curtain came in 2018, when researchers at Lookout Security Intelligence uncovered a campaign targeting government officials, including diplomats and military in Pakistan, Afghanistan, India, Iraq and the UAE.[53] The targets included activists, and some collateral collection also took place involving US, Australian and German government officials. Lookout attributed the campaign to the Pakistani military – and observed that it relied on compromising mobile devices with Android and iOS operating systems. Much of the observed activities involved intelligence collection from the targets.

Lookout also noted that they observed spyware tools offered for commercial sale sharing some similarities with the tools used by the Stealth Mango and Tangelo groups – which is another example of the easy transfer of knowledge and technology between nation-state groups and commercial hackers.[54] A side benefit of the commonality in the types of tools used – as the Lookout researchers noted – is that the compromise of these tools does not carry the cost that is often required to exploit an unknown vulnerability, a so-called zero day. This likely makes the threat actors far more willing to deploy the tools more aggressively.[55]

---

[52] The Economic Times (2018, July 14). *India Is Quietly Preparing A Cyber Warfare Unit To Fight A New Kind Of Enemy*. Retrieved from: https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-a-new-warfare-unit-to-fight-a-new-kind-of-enemy/articleshow/61141277.cms?from=mdr

[53] Blaich, Andrew and Michael Flossman (2018, May 15). Lookout. *Stealth Mango And Tangelo: Nation State Mobile Surveillanceware Stealing Data From Military & Government Officials*. Retrieved from: https://blog/lookout.com/stealth-mango

[54] ibid.

[55] Curits, Franklin (2018, July 26). DarkReading. *Stealth Mango Proves Malware Success Doesn't Require Advanced Tech*. Retrieved from: https://www.darkreading.com/endpoint/privacy/stealth-mango-proves-malware-success-doesn't-require-advanced-tech/d/d-id/1332408

Acknowledgements

When we began this project, the grand scope of the question challenged us to narrow, define, and refine - without forgoing this unique opportunity - to bring a fresh perspective on an emerging trend.

This team would like to thank the Analytic Exchange Program organizers, specifically, Tammy Padilla and her team, for their stewardship in tackling this broad, complex topic. We appreciate the support of the Department of Homeland Security and the Office of Director of National Intelligence - AEP is a leading exemplar of public-private partnership and innovation in intelligence.

Any errors or analytical shortcomings are our own, and do not represent our respective organizations. We are grateful to the individuals and organizations listed below for their contributions, whether insight, comments, or contacts. We spoke and interacted with over 50 experts across sectors, and for privacy and security reasons, not all of them are named here.

We hope that this partial list reflects the diversity of the contributors to this product, while also acting as a reminder that many of those who provide service don't ask for credit.

Andrea Limbago Chief Social Scientist Virtru	**James Mulvenon** SOS International	**Robert K. Knake** Northeastern University
Catherine Lotrionte Georgetown University	**Jason Healey** Senior Research Scholar Columbia University's School of International and Public Affairs	**Steve Brown** National Crime Agency, United Kingdom
Chris Hurst Stabilitas	**Jeff Fields** Supervisory Special Agent Federal Bureau of Investigation (FBI)	**Tim Maurer** Cyber Policy Initiative Carnegie Endowment for International Peace
David Forscey Aspen Institute	**John Fant** Peraton	**Troels Oerting** Chairman of the Advisory Board of the Centre for Cybersecurity World Economic Forum
David Gioe Army Cyber Institute, West Point	**Kevin Allison** Eurasia Group	A Large Financial Institution

Duncan Hollis Temple University School of Law Carnegie Endowment for International Peace	**Laura Galante** Galante Strategies	A US geopolitical risk advisory firm
Erica Borghard Army Cyber Institute, West Point	**Nicole Eshenbaugh** Kroll Cyber Risk	Federal Bureau of Investigation (FBI)
Galina Antova Claroty	**Nina Kollars** Associate Professor Naval War College	Large Global Investment Bank
Harvey Rishikof Senior Counselor ABA SCOLANS	**Omar Khawaja** HM Health Solutions, Inc.	Simon Everett, Ltd.
James Bosworth Founder Hxagon, LLC.	**Pablo Breuer** Sofwerx Donovan Group, US Special Operations Command	The National Cyber-Forensics and Training Alliance (NCFTA)
University of Pittsburgh Institute for Cyber Law, Policy, and Security.		

Commodification of Cyber Capabilities Team Members

Munish P.	US Government
Megan Foster	FS-ISAC
Kyle H.	US Government
Dana M.	US Government
Suzel S.	US Government
Guillermo Christensen	Ice Miller LLP
Pipps Nash	
Tony Porter	FON Advisors
Aaron Henry	FireEye
Clare Boyle	US Government