How Could They Not: Thinking Like a State Cyber Threat Actor

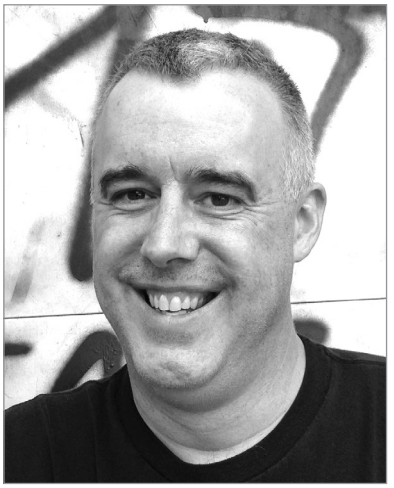
Gregory Conti
Robert Fanelli

ABSTRACT

Information security and intelligence professionals have long known the value of thinking like their adversary. If the defender can put themselves into the mind of their adversary, they can predict behaviors, anticipate attacks, and make moves and counter-moves that frustrate their enemy at a level far beyond what a traditional reactive defense can accomplish. While much has been discussed about cyber threats in general, state actors are a special case with unique attributes. In the press we see coverage of state cyber operations, but only at the surface level. This article provides a more meaningful, and ultimately more useful, understanding of how state actors think, what incentives drive them, what challenges they face, and what special advantages state actors possess.

INTRODUCTION

One of the most valuable information security skills is thinking like an adversary. However, not all adversaries are created the same. Defenders who do not understand how state cyber forces operate can come to false and potentially dangerous conclusions about the risks they face. Conversely, by knowing how a state cyber force thinks, their capabilities, bureaucracy, constraints, incentives, and ultimately how they view the world, we can develop better defenses against these the most capable of all threat groups.



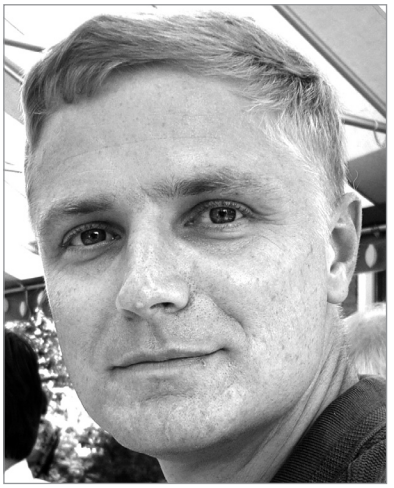
Gregory Conti is Senior Security Strategist at IronNet Cybersecurity. Previously, he ran West Point's cybersecurity research and education programs for almost a decade and served in a career of intelligence and cyber operations assignments. He holds a PhD in computer science and has published more than 70 research articles covering cyber warfare, online privacy, usable security, and security data visualization. He is co-author of the recently published book – On Cyber: Towards an Operational Art for Cyber Conflict. Greg has served as Officer in Charge of a forward deployed expeditionary cyber team, acted as a Senior Advisor in the US Cyber Command Commander's Action Group, and co-created U.S. Cyber Command's flagship Joint Advanced Cyber Warfare Course (JACWC). He has spoken at numerous security conferences, including Black Hat, DEFCON, ShmooCon, RSA, and the NATO Conference on Cyber Conflict and numerous academic conferences. His work can be found at www.gregconti.com and @cyberbgone

Having worked at both the National Security Agency (NSA) and U.S. Cyber Command (USCYBERCOM), the most valuable learning points for us weren't the tools and tactics of today's threat actors, but how they think. We saw a first-hand glimpse of NSA's Tailored Access Operations (TAO) in Rob Joyce's powerful USENIX Enigma talk two years ago. This talk gave us clues into how his team thought about cyber operations.[1] This article extends these insights by highlighting what makes state threat actors different, how they think, and how we can blunt their activities by crafting better defenses.

The line between the capabilities of state cyber forces and those of criminal groups is blurry. There are both sophisticated criminal groups and lousy state groups today. This has not changed. However, state cyber forces have unique capabilities that criminal groups do not possess. States employ the full extent of national power in ways even the most sophisticated criminal groups simply cannot.

Tools like the Center for Internet Security's Top 20 Controls and the NIST Cybersecurity Framework are effective means to help construct defenses against the most common 80% of threats.[2] However, the CIS Top 20 and NIST Cybersecurity Framework[3] alone will not stop the dedicated and well-resourced state actor. Covering that 20% gap is the true challenge. While we aspire to perfect security, we can never reach it, even with extensive resources and attention. We can, however, accomplish much by understanding the state threat and crafting our defenses accordingly.

Of course, no two nations are the same. How a liberal democracy thinks about cyber operations may differ greatly from an authoritarian regime. Even within these general classes, the unique attributes of each country, its culture, and its objectives may vary dramatically. To account for the differences, we have distilled underlying principles that are broadly applicable.



Robert Fanelli is a computer scientist and security practitioner with IronNet Cybersecurity. Prior to joining IronNet, he served as a US Army Colonel at U.S. Cyber Command in multiple roles, including controlling DoD global cyberspace operations, leading the USCYBERCOM/NSA Combined Action Group and conducting research and development activities. He has published, presented and taught security topics in several venues, including the United States Military Academy at West Point and the National Cryptologic School. He holds a PhD in Computer Science from the University of Hawaii, MS from the University of Louisville, a BS from Penn State University, and several industry credentials, including the designation of GIAC Security Expert (GSE).

State Activities Aren't Always State-Only

We tend to think of state cyber operations as unilateral activities, but the reality is more complicated. Operations may be state-operated, state-sponsored, state-affiliated, or state tolerated.[4] States may prohibit, ignore, encourage, shape, coordinate, order, or execute cyber activities.[5] As these nuanced relationships imply, partnerships, either willing or coerced, are common.

A state may provide targeting data to patriotic hackers, immunity to criminal groups, advanced tools to mercenaries, protect a leaker from extradition, or collect intelligence via state-owned technology companies. By operating through explicit or implicit partnerships states hinder attribution and gain plausible deniability for their activities. Expect partnerships between states and less capable, often disposable, threat actors. When you see non-state groups conduct cyber operations with an unlikely degree of sophistication, consider if there is a state benefactor behind the scenes.

State Actors Can Be Unreasonably Tenacious

State backing provides advantages that permit state actors to explore further, delve deeper, and persist longer than other actors in pursuit of their objectives. The assertion that a strong enough defense will dissuade attackers and induce them to go elsewhere in search of a softer target will not hold up when targeted by state actors.

State sponsorship provides more extensive access to hardware, software, infrastructure, and other resources needed to conduct operations. State actors can apply these resources to find and exploit vulnerabilities that other actors would bypass as being too difficult or uncommon to be worth the effort. State actors can also apply resources to conduct coordinated operations on multiple targets simultaneously. A single successful operation may be enough to achieve the overall objective. Further, resources expended during operations can be more easily replaced, allowing state actors to keep coming back long after other actors would become significantly impaired or defeated altogether.

Many cyberspace actors conduct their activities on a part-time basis, needing to engage in other work to pay the bills. More committed criminal actors may make a living from their activities, but they must make a profit or move along to another target. State actors have jobs too: to accomplish the state's objectives. Having the bills paid allows these actors to persist in gaining and maintaining access to a target long after the other actors would give up in search of more lucrative opportunities.

Although the potential for profit may not be immediately obvious to defenders, criminal actors typically conduct their operations with some sort of financial gain in mind. Unprofitable operations do not pay the bills and will be discontinued. State actors can pursue extensive operations with no opportunity for financial gain because profit is not the objective.

A tenet of information system security is that should a vulnerability exist, sooner or later an intruder will find and exploit it. State actors have the tenacity to find and exploit vulnerabilities in ways, and over time frames, that are not feasible for others.

States Create Vulnerabilities

Most attackers use pre-existing vulnerabilities to conduct their attacks, more sophisticated attackers find new vulnerabilities to exploit, but the most sophisticated—state attackers—will create their own vulnerabilities.[6] State actors use publicly available tools and techniques first. Public techniques are cost effective, reduce the chance of attribution, and avoid leaking sensitive tradecraft. Using a novel capability is expensive and risks revealing the attack, mode of operation, and providing incriminating clues for attribution.[7] Copycat tools and resistant defenses would soon follow.

At the next tier, states discover new vulnerabilities. While independent hackers may perform vulnerability discovery,[8] the key difference is scale, scope, and access to prohibitively expensive gear, such as x-ray machines, electron microscopes, and other equipment needed to emulate their target. While a small group of hackers seeking to identify vulnerabilities might purchase used parking meters on discounted websites,[9] they could not muster the resources to build a small nuclear centrifuge facility.[10] Sophisticated states employ massive vulnerability discovery efforts, such as employing contractors who specialize in large scale fuzzing, paying large sums of money to bug bounty hunters, and acquiring access to proprietary source code and hardware designs.

States are effectively unique at the highest tier—creating vulnerabilities. Such activities are rarely attributed publicly, but we see echoes and accusations reported in the press. For example the US banned the use of Kaspersky technologies in the federal government due to concerns over Kremlin influence.[11] The long-standing tension between the US government and Chinese technology companies ZTE and Huawei come from similar concerns.[12] The US government has been accused of deliberately weakening the Data Encryption Standard (DES)[13] and paying a security vendor $10M to weaken its flagship security product.[14]

State actors exploit privileged relationships with companies under their influence. Such relationships can lead to supply chain attacks that compromise hardware or software before the technology even leaves the factory. Even if the company is unwilling, access to desirable markets is another a means of creating vulnerability. For example, to comply with China's cybersecurity laws, Apple moved iCloud cryptographic account keys and customer data into China.[15] Similarly, Google moved servers and user data to Russian data centers to comply with Russian law.[16] We should assume states will maneuver security sensitive devices, people, hardware, software, companies, standards, and information to create vulnerability.

State Cyber Forces Will Push the Limits of Authority

State cyber forces want to aggressively do their jobs and will push their authorized activities to the limit, and then ask for greater authority.[17] A good analogy is that of a guard dog: the guard dog will strain against its chain. Give it a longer chain—sometimes wise and sometimes unwise—and it patrols a larger area. Many of these legal authorities will not be publicly acknowledged, but quietly overseen by government officials.[18] There is a difference between "legal" and "front page of the New York Times legal," though, so some legal authorities may be undermined or eliminated if they become public.

Going Off Script Can Get Operators Reprimanded, Banished, Imprisoned…or Promoted

Whether long or short, every government has a leash on its cyber forces. The degree varies by the type of government and affects both operations and the personal lives of operators. Failure to comply invites punishments that vary based on culture and rule of law. In law-abiding democracies, we'll see career terminations, reassignments, and arrests. In strict regimes, we'll see more severe punishments, including execution. As an example, German hacker, Karl "hagbard" Koch, who allegedly worked for the KGB, was found burned to death after a computer espionage operation ended badly.[19]

In traditional military operations, the US employs the Mission Command paradigm, which pushes authority and responsibility down to those at the front lines, which creates great agility and responsiveness. In contrast, the Soviet military maintained tighter hierarchical control, limiting their agility. Today, the US maintains tight control of cyber operations while many other threat actors maintain a looser degree of control. With less control, cyber operations can be executed and adapted more rapidly.

Cyber force personnel are also under control and observation. The more sensitive the work of an individual, the more intense the scrutiny. It is common to require operators to undergo extensive and reoccurring background checks and polygraph exams. As the frequency of these checks may be insufficient, the US is exploring continuous monitoring of clearance holders—checking such things as court proceedings, financial data, and credit scores for anomalies in near real time.[20]

Not all failure ends in doom. "Fail fast" is a philosophy common in Silicon Valley and is increasingly fashionable in militaries. Innovation is necessary for success in cyber conflict and innovation can't flow when organizations are rigid and risk adverse. At a recent cyber conflict panel, Katie Moussouris asserted that, "we need rule-following rule breakers."[21]

Hierarchical bureaucracies don't readily embrace innovation and rule breaking, but those that do gain the advantage. The US does not possess a monopoly on innovation. As the secrecy of the Democratic National Convention hack unraveled, those behind the operation agilely created the Guccifer 2.0 persona to share the leaked documents—turning the beginnings of a defeat into a victory. We are seeing a shift in the cyber activity in Asian countries move from intellectual property theft to entrepreneurship. We should expect increasing innovation from the state cyber forces of all countries.

No government likes to be embarrassed by its cyber operations. With flexibility comes innovation, but also risk. Because of the risks, expect a playbook of authorized activities and step-by-step scripts of actual operations from nations that enact strict control. In nations employing looser command and control, there will still be boundaries, such as avoiding hacking internal to the country and avoiding embarrassment to government officials.

State Actors Challenge Fundamental Security Assumptions

State cyber actors adeptly exploit security assumptions. We all make assumptions about the security of our systems, the risks we face, and threat actor abilities. When our assessment is off, we can expect a bad day. For example, most users assume their web communications are secure. In actuality, web security is based on cryptographic certificates embedded in our browsers. This assumption proved dangerous in 2011 when a state threat group breached Dutch certificate authority, DigiNotar, issued fraudulent certificates and conducted a large-scale man-in-the-middle attack against Iranian Gmail users.[22] Another core security technology, code signing, designed to prove authorship of software, was similarly utilized to create authentic appearing, but malicious software.[23] According to press reports, state actors may have created sham academic conferences to lure potential defectors,[24] installed malware in hard drive firmware,[25] partnered with chip manufacturers to create hidden back doors, and threatened undersea telecommunication cables with submarines.[26] Whether these specific examples, supply chain attacks, compromising insiders, or something that we have yet to consider, states will not necessarily fight "fair"—even if at the cost of the broader security ecosystem. We must carefully consider the security and trust assumptions we make about state threats.

States Actors Have Strategies; We Have Tactics[27]

Sophisticated state actors execute long-term plans, while most defenders are perpetually stuck in near-present tactics. State strategies aim for long-term objectives, like creating division in the US or undermining US dominance in the world. Multiple supporting operations and campaigns,[28] cyber and otherwise, support the implementation of such strategies. Leaders in

democratic governments—those charged with lasting strategy—have difficulty creating long-term defensive programs. Each politician's influence is at risk every election cycle so long-term planning suffers. The private sector often suffers from similar limitations, as the average tenure of corporate security executives and directors hovers around 2.5 years.[29]

Short range thinking at both the enterprise and national-level hinders defense. We often hear of a looming cyber-Pearl Harbor, but a death-by-a-thousand-cuts scenario is happening now. Patient threat actors operate below a threshold of national response—the type of attacks that cause damage or public outcry that demand a response. Consider the U.S. Office of Personnel Management (OPM) hack of 2015. Significant as it was, years later little has changed.[30] Accountability in the private sector is not much different. A year after the Equifax hack, the company has yet to face serious consequences.[31]

Government lethargy gives state attackers the space to execute strategies over years. Occasionally actors do cross the line and generate more than a token response. But these incidents are rare. Russian influence operations during the US presidential election clearly got the attention of policymakers, but even so, the wheels of government turn slowly. Absent a painful and long-lasting deterrent, threat actors continue with their long-term plans. Success emboldens future audacious activity.

Expect long-long term planning conducted by professional cyber operators, intelligence analysts, and military planners. Some plans are used immediately, while others sit on the shelf until needed. Central to the success of many cyber operations is privileged access to target computing systems. Governments will cultivate such access over many years. Some access will be used to quietly gain intelligence and others will be maintained for later use in time of crisis or opportunity. State actors conduct systematic reconnaissance to keep their plans fresh. Analysts will use intelligence community tools like Center of Gravity[32] analysis, which breaks anything down—from a country to a sector to an enterprise—into vulnerable parts, to build prioritized targeting lists. These lists guide intelligence collection efforts and offensive action. The acquisition of access and the conduct of surveillance occurs continuously as do cyber operations that fall below the threshold of an organized response.

Defenders cannot play checkers while are adversaries are playing chess. States execute synchronized strategies across many playing boards: political, economic, informational, social, and technical, and plan many moves ahead.

States Think at Massive Scale

States think big. When individuals and small groups can quickly create tools that scan the entire internet in minutes (MassScan),[33] massive databases of compromised accounts (Have I Been Pwned),[34] a hardware-based code cracking machine (DES Cracker),[35] a search engine for internet-connected devices (Shodan),[36] a platform for easily organizing and employing computer exploits (Metasploit),[37] and a small computer program that combines Metasploit

and Shodan into a weaponized targeting and exploitation platform (Autosploit),[38] we should assume sophisticated states are more capable by an order of magnitude or more.

Ask yourself what could you do with a billion-dollar budget, a robust intelligence apparatus, a cyber army, and sovereign immunity? Maybe repeatedly map the entire Internet, create special forces-like A-teams for offensive and defensive operations, develop a global targeting database, call every phone number on the planet looking for connected technology and vulnerable humans, optically scan the outside of every piece of mail in a postal system, weaponize artificial intelligence, compromise election infrastructure, work with printer vendors to place covert microdot serial numbers on printouts, use submarines to probe undersea cables,[39] or plant malware in critical infrastructure. Or maybe, steal a database of every security clearance holder in a country (OPM Hack), combine it with their travel records (United Airlines Hack) and medical health information (Anthem Hack), and then build a Facebook-like interface for easy navigation by your spies and cyber operators?[40]

Those who think they aren't a state target are wrong. If you are doing something of value, you are on a state targeting list. If you are really interesting, like a critical infrastructure company or a senior official, you'll get extra attention.

States Have Security Research Ahead of the Open Community

Much state security research occurs behind closed doors. We should assume that state cyber forces are five to ten or more years ahead in cryptography and offensive security. One famous example is that of public key cryptography. From 1970-1973, the UK's GCHQ covertly developed public key cryptography. Academic researchers later discovered public key cryptography in 1976. GCHQ's classified discovery did not become known until it was declassified 27 years later.

Governments invest billions into classified and unclassified research programs. US programs like DARPA's Cyber Grand Challenge[41] used AI to attack and defend machines and the Neural Engineering System Design program which seeks direct communications between digital technology and the human brain.[42] Not all countries have the will or resources to fund such massive programs, instead they may simply steal the intellectual property. We should assume foreign cyber powers have well placed faculty members and students across US academic institutions, seek to place agents in private sector companies, and use leading information security conferences to gather information and recruit.

While classified programs lead in many areas, especially offense, private industry leads in others. Many top companies have well established operational cyber defense programs that provide best practices. That said, less well-resourced small and mid-sized companies lag behind these benchmarks, as does much of the government sector outside of the defense and intelligence communities.

We must move beyond US overconfidence and assume we will not enjoy a perpetual lead in many emerging technologies. For example, China has made major advances in quantum computing,[43] supercomputing, and artificial intelligence and now rival these technologies in the US. We should expect more.

States Leverage the Full Spectrum of National Power

State cyberspace operations do not exist solely in a technical-only vacuum. Governments employ their full spectrum of tools including diplomatic, informational, economic, law enforcement, and military levers of power to achieve their objectives. A state might ban use of foreign-made technologies or track funding behind suspicious technology transfers, require a tech titan's data be hosted in their country, and exploit state-owned businesses to gain privileged access to data, product specifications, and emerging technologies. Militaries will complement cyberspace operations with air, land, sea, space, electronic warfare, and information operations forces. States possess robust intelligence agencies with global human intelligence, signals intelligence, imagery intelligence, and other collection programs to inform current cyber operations and prepare for future conflict. States can selectively create, enforce, or ignore their laws. A government could issue a state department demarche, create fake passports and manufacture identities, or represent their equities in international policymaking forums. All of these are capabilities out of reach of traditional cyber threat actors. Thus, cyberspace operations themselves will also take place in multiple planes, buttressed by the full range of tools available to national governments.

State Forces Aren't Superhuman

Although we recognize and have addressed many of the strengths of state cyber forces, but these forces are not ten feet tall and bulletproof. Cyber forces today are in fact fragile; they are composed of people with rare talent, operating under intense pressure, and competing for scarce resources.

With size comes bureaucracy, and with bureaucracy comes friction. As a threat actor's size grows, it becomes unwieldy, and efficiency suffers. Here are some examples. Cyber exploits provide a competitive edge and organizations may overclassify their most valuable capabilities to prevent use by internal rivals. Established institutions, such as land and air forces, may see cyber forces as competitors who threaten their power, prestige, personnel, and funding.

Cyber forces are composed of humans and will struggle to attract, train, and retain talent.[44] Good people will leave, get sick, fail a physical fitness test, burn out, have babies, be skipped for promotion, lose their security clearance, or get enticing job offers outside government. Technically talented operators will become frustrated by spending long hours creating briefings to justify their missions. Criminal indictments will dissuade talent from participating in missions.[45] Leaks and compromises will hurt morale and damage public opinion.

Building cyber armies takes time. From the initial directive to create USCYBERCOM in 2009, it took until 2018 for the 133 teams of the command's Cyber Mission Force (CMF) to be fully operational.[46] And this was fast: it was jumpstarted by partnering with NSA and a pool of ready military and civilian talent that existed, in part, due to NSA's Centers of Academic Excellence program established in 1999. During the nine years from inception of USCYBERCOM to a fully operational CMF, the geopolitical and technical landscape shifted continually but the "under construction" force was conducting operations throughout this period. The takeaway: read reports of countries creating cyber armies seemingly overnight with a skeptical eye.

Government agencies—and the teams within agencies—do not necessarily talk to each other. Communication between cyber organizations, kinetic forces, and policymakers will remain problematic as each group struggles with need-to-know security considerations and a lack of shared vocabulary. The churn in civilian and military senior leadership means cyber operators must regularly re-educate and justify their activities to new leaders.

No nation is immune to the effects of politics. Politicians will inject politics into cyber activities—from funding to base locations to legal authorities to oversight. Some good people won't get promoted because they angered the wrong politician, and some less qualified people will be promoted because they have befriended the right person in power. Embarrassing a policymaker will negatively impact cyber activities and threaten cyber leaders; successes will gain accolades.

All governments are ultimately accountable to their populations. Cyber operations may be unpopular, especially those that involve surveillance and privacy. Undermining popular support can undermine governmental cyber operations. Due to the sensitive nature of cyber operations, compounded by a culture of secrecy, many cyber organizations struggle to communicate with their populations and the global audience. Reality on the inside may differ substantially from what is seen in the press.

State cyber forces are at a cultural disadvantage. Foreign adversaries are by definition, foreign. Cyber forces often do not possess the language skill of their targets. In fact, they need to maintain a diverse set of language skills sufficient for each target country, which is no easy feat. Language skills are highly perishable and subtle nuances in language can give away deception attempts. We have all seen this in email spam. Additionally, foreign adversaries lack the deep knowledge of a target country's culture. Experts in desired language and culture may exist, but they are always limited in number.

Finally, operational secrets rarely remain secret. The use of each capability leaks insights to the target, sometimes even a blueprint of the code itself. Cyber tradecraft and tools will be reverse engineered, copied, and improved upon. Obfuscation techniques are not bulletproof. We even see clues of threat actor bureaucracy in malware.[47]

CONCLUSIONS

All too often we underestimate the goals, capabilities, resources, tenacity, and time horizons of state threat actors. The standard best practices espoused by NIST and the CIS Top 20 are an excellent start but fall short of proper state-grade defenses. We can address this gap in a variety of ways:

- **Urgency** – We need to avoid the complacency associated with partial solutions and move with a sense of urgency toward strong defenses.
- **Collective Defense** – Individual companies can't take on state actors individually. Even if one company has strong defenses, a state will patiently probe the business' entire ecosystem, or even the entire business sector, seeking a point of vulnerability until they find one. We need network visibility, automated information sharing, and security orchestration between companies, sectors, and governments to provide a comprehensive defense.
- **Public/Private Partnership for the Offense** – For most companies, it is illegal to hack back. Regardless of legality, corporate hacking back is unwise. Governments possesses a monopoly on the use of force and public/private collaboration is necessary to strike back using the full spectrum of governmental power. A solid collective defense foundation will allow high-speed, automated requests for government support.
- **Realistic, Informed Assumptions** – Recalibrate your security assumptions using an informed and justifiably paranoid view of state threats.
- **Organizational Agility** – Smaller, more agile groups with less systemic friction will respond faster than a large hide-bound force. We must work to reduce bureaucratic friction to increase agility and improve morale.
- **Move Beyond Signature-based Security** – Sophisticated adversaries today avoid detection by signature-based security systems. We need more advanced technologies that detect threat behaviors. While it is easy to bypass signatures, it is much more difficult to bypass a behavioral detection system, such as network behavioral analytics. Deception technologies provide another powerful technique. You own the network, exploit your home field advantage.
- **Cyber National Training Centers** – Governments and companies need to learn how to fight in cyberspace as a cohesive whole. This requires common doctrine, interoperability, information sharing, regular exercises, and trust. Look to the U.S. Army's National Training Center[48] as a model for building strong integrated teams from disparate parts.
- **Military Strategy and Tactics** – Traditional information security controls are insufficient. State cyber forces are far more capable and organized to be deterred by these limited defenses. There are literally armies operating in cyberspace, and armies conduct cyber operations at scale. We must selectively draw from military doctrine for best practices to defend at scale.[49]

Once computing was the domain of hobbyists and well-intentioned hackers. Those days are long past. Cybersecurity today is serious business. Nations compete for dominance, and cybersecurity is looking a lot more like warfare, and business as usual is simply insufficient. No company can stand alone against state threat actors. Ignoring that states are active in cyberspace will not make the problem go away. For all their strengths however, state threat actors do possess weaknesses we can exploit. The CIS Top 20 Controls and the NIST Cybersecurity Framework provide the foundation for a credible defense, but they are insufficient alone. An urgent and rapid response that factors in state actors is necessary. We must learn to defend as sectors and nations in tight coordination.

Learning to think like a state actor is the fundamental first step. For defenders, the most important takeaway for understanding a state actor isn't "would they do it" or "could they do it," but instead, "how could they not?"

DISCLAIMER

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, Department of the Army, Department of Defense, the National Security Agency, U.S. Cyber Command, the United States Government, IronNet Cybersecurity, or any other current or past employer.

NOTES

1. Rob Joyce, "Disrupting Nation State Hackers," USENIX Enigma, 2016, https://www.usenix.org/node/194636. See also, Rob Joyce, "NSA Talks Cybersecurity," DEFCON, 2018.
2. "CIS Controls," Center for Internet Security, https://www.cisecurity.org/controls/.
3. "Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework.
4. Mara Tam, Twitter, August 29, 2018. https://twitter.com/marasawr/status/1034856944090206208
5. Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Atlantic Council, January 2012.
6. U.S. Department of Defense, "Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board Task Force Report, 2013.
7. The use of a novel capability is sometimes called a "use-it-and-lose-it OPSEC risk."
8. Sean Michael Kerner, "Critical Bug Bounty Reports on the Rise, HackerOne Finds," eWeek, July 12, 2018.
9. Joe Grand, Jake Appelbaum, and Chris Tarnovsky, "Smart Parking Meter Implementations, Globalism, and You: aka Meter Maids Eat Their Young," DEFCON, 2009.
10. Kim Zetter, Countdown to Zero Day, Broadway Books, 2015.
11. Dustin Volz, "Trump signs into law U.S. government ban on Kaspersky Lab software," Reuters, December 12, 2017.
12. Ginger Gibson, "U.S. House passes defense bill targeting Chinese investments," Reuters, July 26, 2018.
13. Bruce Schneier, "The Legacy of DES," Schneier on Security, 2004.
14. Dennis Fisher, "RSA Denies NSA Backdoor Payment Allegations," Threatpost, December 23, 2013.
15. Mikey Campbell, "Apple to move Chinese iCloud keys to China servers, opens door to government data requests," AppleInsider, February 23, 2018.
16. Olga Razumovskaya, "Google Moves Some Servers to Russian Data Centers," Wall Street Journal, April 10, 2015.
17. Dakota Rudesill, "Trump's Secret Order on Pulling the Cyber Trigger," Lawfare, August 29, 2018.
18. Alex Boutilier, "Canada's electronic spies will be able to launch cyber attacks with little oversight, report warns," The Star, December 18, 2017.
19. Cliff Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Pocket Books, 2005.
20. Patrick Tucker, "US Plans 'Continuous Evaluation' of New and Existing Security Clearances," Defense One, July 12, 2018.
21. Adin Dobkin, "Army pushes recruiting and retaining cyber talent," Defense Systems, November 8, 2017.
22. Dennis Fisher, "Final Report on DigiNotar Hack Shows Total Compromise of CA Servers," Threatpost, October 31, 2012.
23. Dan Goodin, "Stuxnet-style code signing is more widespread than anyone thought, ArsTechnica, November 3, 2017.
24. Daniel Golden, "How the CIA Staged Sham Academic Conferences to Thwart Iran's Nuclear Program," ProPublica, October 10, 2017.
25. Sean Gallagher, "How hackers could attack hard drives to create a pervasive backdoor," ArsTechnica, February 18, 2015.
26. Garrett Hinck, "Evaluating the Russian Threat to Undersea Cables," Lawfare, March 5, 2018.
27. Derived from Jeff Moss' comment "our adversaries have strategies, we have tactics" in Black Hat USA Keynote Introduction, 2018.
28. Richard Bejtlich, "Elevating the Discussion on Security Incidents," TaoSecurity Blog, February 19, 2015.
29. "Understaffed and at Risk: Today's IT Security Department," Ponemon Institute, February 2014.
30. Lee Mathews, "Office of Personnel Management Still Vulnerable 3 Years After Massive Hack," Forbes, November 15, 2018.
31. Zack Whittaker, "A year later, Equifax lost your data but faced little fallout," TechCrunch, CNET, September 8, 2018.
32. Dale Eikmeier, "The Center of Gravity: Still Relevant After All These Years," Military Review, May 11, 2017.
33. Robert Graham, MassScan, GitHub.
34. Have I Been Pwned, https://haveibeenpwned.com/.
35. "EFF DES Cracker Machine Brings Honesty to Crypto Debate," Press Release, Electronic Frontier Foundation, August 9, 2016.
36. Shodan, https://www.shodan.io/.
37. Metasploit, https://www.rapid7.com/products/metasploit/.
38. Teri Robinson, "Autosploit marries Shodan, Metasploit, puts IoT devices at risk," SC Magazine, January 31, 2018.
39. Morgan Chalfant and Olivia Beavers, "Spotlight falls on Russian threat to undersea cables," The Hill, June 17, 2018.

NOTES

40. The Grugq, "A Short Course in Cyber Warfare," Black Hat Asia, 2018.
41. "DARPA Celebrates Cyber Grand Challenge Winners," Press Release, DARPA, August 5, 2016.
42. "Bridging the Bio-Electronic Divide," Press Release, DARPA, January 19, 2016.
43. Martin Giles, "The man turning China into a quantum superpower," MIT Technology Review, 19 December 2018.
44. Josh Lospinoso, "Fish Out of Water: How the Military is an Impossible Place for Hackers, and What To Do About It," War on the Rocks, 12 July 2018.
45. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Press Release, U.S. Department of Justice, May 19, 2014.
46. "Cyber Mission Force achieves Full Operational Capability," Press Release, U.S. Cyber Command, May 17, 2018.
47. Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," Smithsonian Magazine, April 2012.
48. Mario Hoffman, "Modernizing the Army's OPFOR program to become a near-peer sparring partner," Army.mil, October 1, 2018.
49. Gregory Conti and David Raymond, "On Cyber: Towards an Operational Art for Cyber Conflict, Kopidion Press, 2017.