

REPORTS & PAPERS

from **Cyber Security Project**, Belfer Center

The Legend of Sophistication in Cyber Operations

Published:

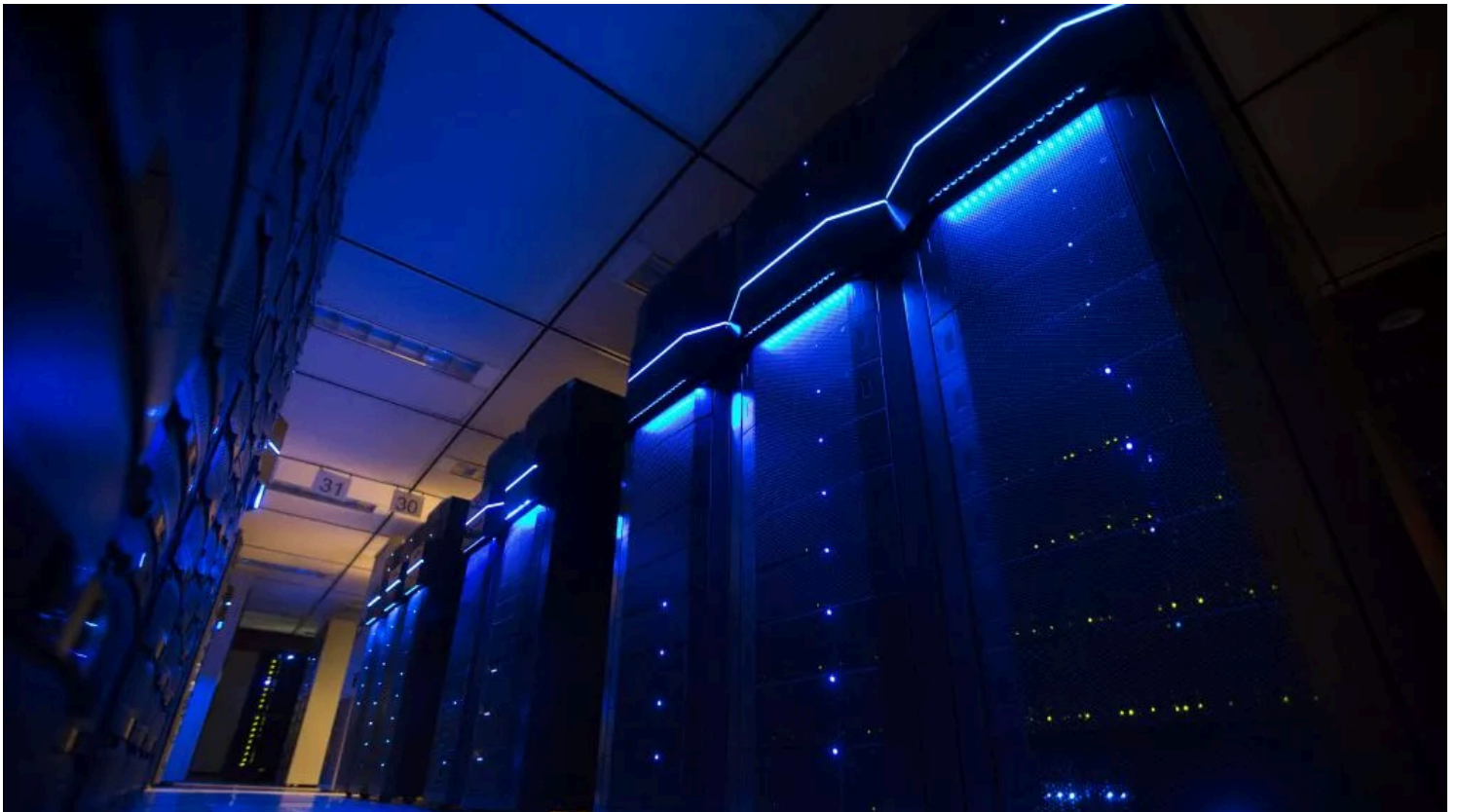
January 2017

Author

Ben Buchanan

Related Programs

Cyber Project





Server racks inside a data center at American Electrical Power headquarters in Columbus, Ohio, May 2015

Executive Summary

In a drumbeat of news stories and corporate press releases, one phrase has dramatically grown in use over the last decade: “sophisticated cyber attack.” These words have been used to describe specific intrusions into telecommunication providers, insurance companies, social media hubs, banks, the Pentagon, a host of security firms, government agencies, research labs, movie studios, and much more. It seems the world is awash in sophisticated network intrusions.

But if everything is sophisticated, nothing is. This paper unpacks “sophistication” in cyber operations, exploring what it means, and what it should mean, for an operation to attain such a status. It examines the incentives for victims and observers to overstate the sophistication of other actors. Additionally, it offers a more rigorous framework for defining the term that takes into account technical and operational factors. But deploying the lens of sophistication by itself can be misleading; this paper also explores the incentives some actors have to deploy less sophisticated capabilities.

From this foundation, the paper concludes by linking sophistication to overarching questions of theory and practice in cyber strategy. It shows how a sharper understanding of the notion of sophistication calms some worries about asymmetric cyber capabilities; defense is doable. It examines as well how sophistication bears on the applicability and utility of the offense-defense balance in cyber operations, an area of both academic and policy debate. All told, for scholars and practitioners, this paper offers a path forward to more rigorously analyzing modern cyber operations.

The Legend of Sophistication in Cyber Operations

In February 2015, Kaspersky Lab exposed “Equation,” a group of hackers that carried out operations all over the world. The Equation operators drew praise from Kaspersky’s analysts for their technically impressive tradecraft. The forensic analysts called them “one of the most sophisticated cyber attack groups in the world, and probably the most advanced threat actor we have ever seen.”^[1] The analysts noted the operators’ impressive encryption methods, their ability to compromise deeply obscure systems, and their well-developed stable of custom hacking tools. Based on forensic artifacts and corroborating

information in documents leaked by Edward Snowden, it appears quite likely that the group is a division of the United States National Security Agency. ^[2]

Also in 2015, the British telecommunications company TalkTalk suffered a number of network breaches. In August, it disclosed a hack of its mobile sales site that it called “sophisticated and coordinated”; in October, it said another intrusion was the result of a “significant and sustained” cyber attack. The method of entry reportedly employed in at least one of the breaches has existed for many years. In their investigation, police arrested three teenagers and one 20-year old. ^[3]

As divergent as the Equation operations and the TalkTalk hack appear, they were described with similar language. This resemblance is no outlier. Many incident reports and company statements of breaches reference the skill, persistence, and—most often—the “sophistication” of network intruders. Such terminology has fueled news reports, forensic analysts, insurance claims, and plenty of television shows and movies. The idea of sophisticated hackers, whether long-haired teenagers in a basement or well-funded spooks in Fort Meade, has taken on a life of its own. It has become a legend increasingly divorced from fact.

If everyone is sophisticated, no one is. The idea needs more depth than it is usually accorded. A deeper discussion of sophistication can rest on four interrelated questions. First, what does the idea of sophistication mean in the context of cyber operations and what incentives exist to label intrusions as sophisticated? Second, are some operations or tools more sophisticated than others, and how can one tell? Third, are there reasons why a state with the capacity for sophisticated capabilities might choose to launch a less sophisticated operation, or to have less sophisticated components in some of its operations? Fourth, what are the implications of a more nuanced understanding of sophistication, especially for those working at or studying the intersection of cyber operations and international security?

This paper argues that answering these questions, and in the process developing a more rigorous understanding of sophistication, can lead to insights about how cyber operations carried out by states and criminals actually unfold. It can reveal which actors are benefitting from substantial investments in cyber operations, what kind of investments reveal sophistication and specialization, which targets are so vulnerable that they can be breached without sophisticated operations, and what sorts of operations are within the reach of less capable groups. Most importantly, examining sophistication more carefully dispels the legend. It instead reaffirms that not all operations are sophisticated and indeed that defense is doable.

Each of these four questions is the subject of a section that follows. The first section uses better understanding of the concept of sophistication to shed light on the incentives to overhype the capabilities of some intruders. The second section contends that a rigorous technical paradigm coupled with operational assessments of speed, sloppiness, and scope can clarify which operations are in fact deserving of the sophistication mantle. This section introduces a working framework for this kind of

assessment, moving sophistication from a one-dimensional concept to something that is more nuanced. The third section examines why a state might or might not choose to have unsophisticated components in its operations, or might or might not choose to deploy a sophisticated capability.

In the fourth section, armed with greater conceptual depth and more technical rigor, it is then possible to re-examine important strategic debates, such as whether cyber operations might provide an asymmetric advantage for weaker actors, the utility of the offense-defense balance, and whether states can practically promote stability. The conclusion takes stock. It reassesses the ways in which the contemporary understanding of sophistication could be usefully improved, outlining the practical value of a grounded sophistication discussion, and reflecting on the limitations of the concept.

Incentives to Overrate and Overstate Sophistication in Operations

Sophistication is an idea more frequently employed than it is defined. While various dictionary discussions of sophistication refer to complexity and specialized knowledge, in practice sophistication is sometimes reduced to an “I know it when I see it” definition. An operation that is far-sighted, counterintuitive, intricate, and hard to execute deserves the label of sophistication. One that is short-sighted, obvious, blunt, and simple probably does not. This is as true in cyber operations as it is in other affairs of state.

A wide variety of cyber operations are labeled as sophisticated because the definition is ambiguous. Too often, the metric for a so-called sophisticated operation is simply success. If the mission worked, it was sophisticated; if it failed, it was not. But this view is too narrow. One can imagine NSA operations that rely on the agency’s toolkits of advanced network technologies—which seem on the whole to be sophisticated—that nonetheless fail to achieve their desired ends. And one can easily find cases, including the TalkTalk hack, in which comparatively basic operational methods achieved their goal. Success should not equal sophistication.

It is the victim or an observer who most often labels an operation as sophisticated. An anecdote illustrates one end of the spectrum in this respect: The American chess grandmaster Bobby Fischer was one of the most capable and successful people to ever play the game. He was feared for his abilities and sometimes disliked for his arrogance. According to a perhaps apocryphal story, after Fischer dominated another grandmaster on the board, the victim blamed his loss on high-blood pressure and a pounding headache rather than acknowledge a fair defeat to a more sophisticated player. The ever-irascible Fischer, tired of such excuses, is said to have quipped, “I never beat a healthy opponent.”

In important respects, however, the attitude of major organizations when suffering a network breach is on the opposite end of the spectrum. Whereas some 20th century chess players preferred to lament, or even invent, their own failings rather than praise Fischer, 21st century digital victims would rather praise and

hype their opponents' skills. This is true even when those skills are nothing particularly remarkable, and especially when they are successful.

Several incentives encourage this. First, disclosure requirements have begun to mandate that private sector firms reveal when they have been hacked and have lost customer data.^[4] This forces news of a breach out into the open. While this is a good outcome in many respects, the resulting public relations challenges require companies to provide an explanation for an attack and work to retain customers. As part of this effort, many companies are often loath to admit their own failings, preferring instead to overstate the capabilities of the digital intruders. Rather than acknowledge lapses in basic security practice, victim organizations are more likely to claim, sometimes implicitly, that their adversaries were so capable that no reasonable amount of security would have kept them out. They will often employ the language of sophistication in these claims, relying on the fact that the media and public will be unable to parse the nuances.

Second, the economic incentive structure sometimes encourages this kind of behavior. With the rise of cyber insurance, firms suffering a breach often seek to get reimbursed for some of its costs. Though the case and contract law of this area is only nascent, any insurance claim is made more credible when it is clear that the underlying incident is beyond the victim's control. By amplifying the extent of the intruders' capabilities and raising the specter of significant costly damage, firms can increase their chances of an insurance payout. Conversely, admitting a firm's own failures in network security would weaken the case. As the insurance market develops, it is likely this effect will moderate. Nevertheless, at least one experienced analyst reports that this is still a reason for over-hyping breaches; claiming a breach by "[s]ophisticated, advanced, nation-state hackers means money all around."^[5]

Third, observers as well as victims have incentives to overstate the sophistication of activity they uncover. In 2013, the incident response firm Mandiant published a landmark report on a group of hackers that it called "Advanced Persistent Threat 1." Mandiant revealed evidence that indicated the hackers were affiliated with Unit 61398 of the Chinese People's Liberation Army.^[6] The firm's analysis appears solid, though many of the Chinese group's capabilities were not incredibly novel. The report, which came at a time of growing concern about cybersecurity, attracted major media attention. In important respects, it spawned a new genre—sometimes derisively referred to as "Advanced Persistent Marketing"—of public threat analysis. Incident response firms, drawn to the possibility of greater prominence, gained an incentive to publish attention-seeking reports on threats or cases.^[7]

In some ways, the trend started by the APT1 analysis is a very positive one. Some of the work done by incident responders has been rigorous and of high quality, taking care to not overstate facts and to present competing hypotheses. With this work in the public domain, it becomes possible for researchers to learn more about trends in cybersecurity. Other work is less credible. Some firms have drawn sweeping conclusions based on small amounts of data, positing sophisticated false flag attacks where none seem to exist: this was the case with one report that claimed the 2014 cyber attack on Sony was Russian, not

to exist, and was the case with one report that claimed the 2011 cyber attack on Sony was Russian, not North Korean, in origin. ^[8] Other reports have over-hyped particular threats, such as one that claimed Iran was developing sophisticated capabilities for targeting Industrial Control Systems. ^[9] Too frequently, these reports have been repeated uncritically by media outlets. When, in pursuit of marketing and page views, firms and media overstate the capabilities of some actors, the legend of sophistication only grows.

A Working Framework for Sophistication in Cyber Operations

It is possible to more rigorously test the idea of sophistication in cyber operations. Examining technical sources enables the construction of a typology of techniques for key operational components. Analysis of intruders' tools and procedures can identify how varying techniques correspond to different levels of sophistication. In addition, examining three overarching factors strengthens the analysis of sophistication: the intruders' speed, mistakes, and operational scope.

For the more technical part of the framework, this section in part uses the work of David Aitel, a former operator at the NSA and a cybersecurity executive. In 2016, Aitel proposed a method for evaluating cyber operations. ^[10] Though his approach was proposed in the context of a discussion about building up operational capacity and developmental limitations, it is similarly useful when focusing on the question of sophistication.

The framework outlines six components of cyber operations: sourcing of tools, usage of tools, network communications, testing, persistence, and operational security. In each of these areas, the approach provides a spectrum of possible approaches to the component. As one advances along the spectrum, the approaches get more complex, expensive, and likely more effective; to a reasonable approximation, they become more sophisticated.

Figure 1: David Aitel's framework outlines six categories one can use to evaluate the technical components of a cyber operation, or of a state's capacity for cyber operations. These can also be used in an analysis of sophistication. Image Credit: David Aitel.

For example, the component of operational security refers to an organization's capacity to protect the secrecy and effectiveness of its operations, even in the case of partial compromise or discovery. On one end of the spectrum are those actors who do not or cannot invest in operational security. These actors are much more likely to use one set of tools for all of their operations. Tool reuse is cheap, easy, does not require re-training, and enables flexibility; this is akin to a burglar who perfects and repeats a method of operations for breaking into houses. But it also runs the risk that investigators who discover one of the

operations for breaking into houses. But it also takes the risk that investigators will discover one of the operations will be able to use the operators' standardized procedures as a way of finding or linking other cases to the same actor. Since burglars often do not have good operational security, police can perform this sort of analysis to group cases together. Both physical and digital intruders that do not invest time and money in solid operational security bear greater downside risk than those who do.

On the other end of the operational security spectrum are organizations that avoid developing such signatures. These organizations are likely to invest in many different tools with different characteristics. They sometimes change their tactics and tools for each operation, striving as much as possible to isolate each mission from the others. If one operation is detected, the others have a better chance of remaining unaffected. But this comes with a cost in money, time, and complexity. As such, it is likely beyond the reach of an individual or small group. This higher level of operational security is as if a bank robbing crime syndicate used a different team for each break-in, preparing the unique team with a set of procedures and instruments that would only be used for one heist.

Persistence, another component in Aitel's technical framework, also provides an intuitive example of a range of sophistication. The concept refers to operators' technical capacity to maintain a malicious presence in the adversary's computer systems despite the adversary's attempts to remove that presence. This kind of technical persistence should not be confused with operational persistence, in which an adversary shows great determination across many attempts to gain illicit access.

A framework for sophistication can draw useful distinctions by analyzing technical tradecraft in the area of persistence. On the lesser end of the spectrum, operators can employ malicious code that installs itself like a regular application on the target's computer. If the target learns of the operation and removes the program or reinstalls the operating system, the operators will lose access. Most malicious code functions in this way and does not feature complex persistence mechanisms. For hard targets, though, more might be required. One way operators can gain persistence is by burrowing their malicious code more deeply into lower levels of the stack of computing software. Gaining a presence in the BIOS,^[11] which runs before the computer's operating system starts up, or in the code of the hardware on which the operating system depends, enables operators to achieve persistence. These more advanced capabilities, which are much harder to develop and execute, are hallmarks of sophisticated and well-resourced action.

These two technical components of operational security and persistence demonstrate that there is a gamut of sophistication in cyber operations. For the other technical components in Aitel's framework, a similar spectrum can be seen. It is not necessary to examine each part of the framework—or even to accept the framework's particulars—in order to reach this conclusion. Simply put, operators must carry out certain core mission tasks, and the technical ways in which they do so reveal something about the operators, their decisions, and their capabilities. Once greater focus is given to these components, and not just the success or failure of the mission, the differences in sophistication in real-world cases become apparent in a more rigorous way.

In addition to a technical examination of tools and procedures, at least three other overarching areas of analysis can be useful in assessing sophistication. These operational factors are often the result of how the operators employ their tools; each involves a combination of technical decisions. One possible area of assessment is speed. While it is often assumed that cyber operations take place at a very rapid speed, such a notion is much too simplistic.^[12] Sometimes the effects of an operation, such as the execution of code that wipes critical data, are quick, but the operational preparation that enables those effects rarely is as fast. If necessary, finding a vulnerability and developing an exploit can be a time-consuming process; some more complex operations require several exploits chained together. At a minimum, it often takes time to get malicious code into a system and gain access to the final target. In general, the faster intruders are at these tasks, the more they can increase their chances of success. As such, operational speed is likely to be a sign of a more sophisticated and experienced actor: one who has an efficient method of entry, can act on the access gained with minimal delay, and can move quickly to accomplish the operational objective.

Mistakes are a second useful factor in assessing operational sophistication. Operators, like everyone else, make errors. When dealing with something as complex as a computer network, especially a foreign one that is not well understood, oversights and contingencies are inevitable. But, all else being equal, a more experienced, capable, and sophisticated operator is less prone to mishaps, especially of a basic nature. By examining log files and observing techniques, investigators can get a sense, however imprecise, for the skill of the intruders. For example, in a cyber attack against Sands Casino in 2014, intruders wiped many computers but had a poor understanding of the target network, limiting the spread of their destructive target code.^[13] In general, repeated or significant errors are signs of a less sophisticated operational effort.

A final additional consideration in assessing sophistication is the intended scope of the mission. A mission to disable a power grid for a long time is far more complex than one that seeks merely to briefly lock a user out of his or her computer. The more ambitious and difficult the mission, the more sophisticated the operators are likely to be—especially if they are successful. This examination of mission scope need not be limited to effects, but can also include how those effects are achieved. For example, the Stuxnet worm managed to destroy centrifuges over a period of time while remaining hidden to the control system's operators. Such stealthy destruction, especially if it occurs against an adversary with developed cyber defenses, is a good indicator of sophistication.

This technical and operational framework highlights differences in sophistication when it is applied to real world cases. For example, the Equation operators uncovered by Kaspersky Lab used advanced persistence mechanisms in order to preserve their presence on targeted systems. They obtained information on the design of hard drives from the world's 12 leading manufacturers and designed the malicious code that would target the software that enabled those hard drives to function. This software, known as firmware, exists beneath the operating system level and malicious code that targets it is virtually impossible to detect and remove. Even if the target wiped their hard drive entirely and started

virtually impossible to detect and remove. Even if the target wiped their hard drive entirely and started again, the malicious code would persist. Kaspersky's lead researcher noted the impressiveness of the Equation operators' technique in his forensic analysis, saying, "This is an ultimate persistence mechanism, and it has the ultimate resilience to removal. This is a next level of persistence never seen before."^[14]

A malicious software toolkit known as Project Sauron, revealed by Kaspersky and Symantec, demonstrates a similarly high degree of sophistication in operational security. The software pretended to be a password filter used by system administrators, but secretly enabled its operators to copy passwords, encryption keys, configuration files, and much more. The amount of attention the Sauron operators dedicated to trying to isolate their operations from one another is striking. The operators used different operational infrastructure and techniques for each of their targets in what appears to be a deliberate attempt to avoid leaving the same signatures in different locations. In light of this and other design choices, Kaspersky noted that, "Technical details show how [the] attackers learned from other extremely advanced actors in order to avoid repeating their mistakes."^[15] It seems to have mostly worked; Sauron operated for at least five years without public detection.

Against this backdrop, the TalkTalk hack is an example of an operation that looks much more pedestrian at a technical and operational level. Based on the four individuals arrested in connection with at least one of the breaches, those hackers left enough information to get caught reasonably swiftly. They used a timeworn technique, SQL injection, to access sensitive data. While the technique was successful against TalkTalk, it is easily blocked by basic security measures; TalkTalk's failure to take fundamental precautions earned the company the largest fine ever issued by its British regulator.^[16] The hackers' motivations appear to have been the immediate theft of financially valuable information, not the acquisition of stealthy access for long-term collection. On virtually every aspect of the above framework, they rank at the most basic end of the spectrum.

The gulf between the Equation and Sauron cases and the TalkTalk breach shows the range of operations labeled "sophisticated." There does not seem much evidence to indicate that the latter case earned the title. Indeed, the fact that the telecommunications company hyped such an unsophisticated operation underscores the incentives to do so. More sober and neutral examination, such as that done by academics or reputable incident responses companies, should take care not to fall into this trap.

Conserving Sophistication

While the last section's framework for assessing technical and operational sophistication is useful, it is worth thinking as well about broader decisions related to sophistication. It is important to disentangle the notion of sophisticated actors from sophisticated operations. In short, sophisticated actors have

good strategic reason to choose to appear unsophisticated in some of their operations. The net result might be called the conservation of sophistication: the incentives are to use the least sophisticated capability that will get the job done.

One benefit of well-known and comparatively basic tools is that they can save money and time. For most of the key tasks in a simple operation, publicly available code can work. These tools will not be effective for every operation, as they will sometimes be too easily detected or not suited to carrying out certain objectives. But when they are appropriate, operators can use them and save on the cost of developing their own toolkit. Further, if the operators are already familiar with the publicly available tools or frameworks, operators can perhaps reduce training costs and increase operational tempo. Sophisticated tools simply might not be needed and could even be counterproductive.

Using such public tools can also muddle attribution. The code used to carry out cyber operations is one factor investigators use in determining the origin of an operation. By avoiding custom code and procedures in favor of—often less sophisticated—tools and techniques that are widely available, operators can make it somewhat harder for investigators to determine their identity. For example, a noteworthy hacker known as Phineas Fisher said that he depended in large part on publicly available tools.^[17] Such reliance on less sophisticated tools does not make attribution impossible, since investigators have other factors they can examine, but it does complicate the problem.^[18]

Similarly, using such tools can increase operational security. As noted earlier, when the same unique malicious code is deployed against many targets, detection in one instance can lead to a much larger number of operations being uncovered. For example, when the Equation Group was discovered, investigators were able to spot the malicious code in key targets all over the world. Using many different sets of tools, even if each is necessarily cheaper or less sophisticated, can help to mitigate this risk. Even so, this technique does not guarantee secrecy. Project Sauron, mentioned earlier, took great pains to avoid toolchain re-use and still was eventually uncovered on a variety of different systems. But if operators can manage to achieve their objectives with unsophisticated and widely accessible code, they can help preserve operational security.

Lastly, even the most sophisticated actors against the hardest targets do not have an unlimited budget of time and money. Resource constraints and the urgency of important missions are a fact of life in the world of intelligence and military operations. Thus, the most capable operators must still make choices about specialization that are related to their choices about sophistication. In one mission, for example, operators might take great care to test and tailor their code, such as by building replica facilities, sacrificing money and time that might have gone into operational security. Stuxnet appears to have been an example of this. In that case, the operators reportedly had an extensive testbed, but less operational security. At least compared to malicious code that came later, the relative openness of the Stuxnet code enabled a great deal of public discussion.^[19] Another mission may yield a different set of choices, in which operational security is prioritized over testing. Planning ahead and managing these kinds of

tradeoffs are key challenges in modern cyber operations.

For the best actors, then, technical and operational sophistication is a choice, or rather, a series of choices. There is no doubt that for some operations against hard targets, custom toolkits that are in some ways sophisticated will have to be deployed. But ideally such capabilities should only be developed and used when necessary, since building and deploying them in other circumstances risks needless expense, overkill, and blowback. No state can afford to be entirely sophisticated in all respects all the time, and each state must seek ways to conserve sophistication where it can. ^[20]

The evidence bears this out. The Equation operators, like many others, preserved some capabilities for the hardest targets. For example, researchers believe that the apparently-unique persistence mechanism against hard drives was deployed just five times. The principal security researcher examining Equation said that, “Only a very select list of victims receive this. This is one of the most rare modules I have seen because it is so valuable, so they don’t want to expose it....It’s a precious plugin that’s used only in specific cases with somebody very important.” ^[21] While the legend of sophistication fuels a notion that every operation is entirely elite, the reality is that some operations, even by the most sophisticated actors, are deliberately less so.

Why Sophistication Matters for Policy and Theory

Sophistication has always mattered in military and intelligence affairs. It grants greater freedom of action and shapes states’ strategic choices. With a framework for evaluating sophistication now established, and with a discussion of the strategic limits on the idea, it becomes possible to examine how the concept relates to key questions at the intersection of cyber operations and international security. Three deserve particular attention: the degree to which cyber capabilities might yield asymmetric advantage, whether states should try to shift the balance between offense and defense in cyber operations, and whether sophisticated states can in fact do so.

The notion of asymmetric capabilities tops the list of relevant issues. Many have theorized that cyber operations offer states with less resources or overall military capability an opportunity to level the playing field or strike at vulnerable parts of stronger states’ infrastructure. If cyber operations are cheaper, or if sophisticated and powerful cyber operations can be achieved without many years of investment and capacity building, weaker states or even non-state actors will be able to catch up. For stronger states, especially those that rely heavily on computing infrastructure, this can appear to be a major concern. ^[22]

Taken together, greater consideration of sophistication can provide a path to partially easing this worry. If it is indeed the case that more sophisticated capabilities are required for actions against high-security targets, sophistication can become a proxy for effectiveness in these operations. This casts doubt on one

targets, sophistication can become a proxy for effectiveness in those operations. This casts doubt on one part of the concern about asymmetric capabilities: less sophisticated capabilities may be able to exploit or attack less-secure targets, but there are limits on their overall potency. The foregoing model indicates that less sophisticated capabilities are, as a generalization, less likely to be tailored and effective, more likely to be detected, and less likely to persist against solid defenses. It follows that stronger states should, in an effort to thwart lesser actors, focus on deploying solid, even if not spectacular, network defenses. Differences in sophistication matter less when breaching soft targets; it is in the realm of high-end intelligence and attack operations, as opposed to criminal activity or the like, where sophistication is likely to matter most.

In addition, if there is also a meaningful difference in operational sophistication between different actors, then it follows that actors with more sophisticated capabilities will possess greater freedom of action. Because these actors are capable of devoting the time and money to build out more developed capabilities where they are needed, they will be able to act against harder targets in a way that is less likely to be detected. Though no actor will always be entirely sophisticated, actors with more time, experience, and resources will be better able to decide where to specialize and invest.

For example, the billions of dollars and many years invested by the NSA enabled, in part, the sophisticated and specialized suite of tools used in some Equation Group operations. This does not mean that actors like the NSA will always find it advantageous or wise to operate with such high-end tools. Nor does it mean that they will always make the right choices about where to develop sophistication. The careful management of cyber operations remains essential, even with a significant head start. Nonetheless, compared to less sophisticated, less well-funded, and less experienced organizations, the agency has greater luxury and insight in developing and deploying the appropriate advanced tools when it seems necessary. This further undercuts the notion that, on the more sophisticated end of the operational spectrum, lesser actors will be able to keep up. ^[23]

This section's second question, a theoretical one, emerges as a result: do states and organizations that already have an advantage when it comes to cyber operations have an incentive to make action harder? It is perhaps the case that if more capable actors can raise the bar on what is required for operational success—in effect, shifting the advantage to the defender against the attacker—they can limit others' ability to act. In so doing, these actors might also raise the bar for their own operations, requiring greater sophistication in order to achieve the intended mission. This is likely to increase the cost of action but, so long as the actor can clear the threshold, not make cyber operations impossible. In theory, a state that is able to achieve this enjoys relative gains over lesser actors. ^[24]

The notion of offense-defense balance is a key part of answering this question. The idea has a long history in international security, with influential articles noting that, all else being equal, an advantage for the defensive side results in less fear and a more stable system. ^[25] With a defensive advantage, decision-makers do not feel an urgency to attack and indeed are rewarded for waiting for a potential adversary to strike first. In cyber operations, it is an ongoing debate whether the offense or the defense

adversary to strike first. In cyber operations, it is an ongoing debate whether the offense or the defense has the advantage, though the dominant perception is that the offense enjoys the edge. ^[26] Such an analysis likely is too simplistic, however, as cyber operations are multi-faceted; perhaps the offense has the advantage when gaining initial entry due to the prevalence of spear-phishing, for example, but the defense enjoys the edge when it comes to detecting malicious code in well-architected networks.

In general, though, shifting the balance to the defense could help achieve stability desired by states that already have advantages, especially if doing so improves detection and attribution. Cyber operations can be tempting for decision-makers because they offer the allure of covert intelligence collection or action. If the chances of detection and attribution increase, then the operations will appear riskier and perhaps substantially less attractive for weaker and non-state actors. The more strong states can detect the activities of weaker ones, the greater advantages these stronger states will enjoy.

The third and final question follows: even if there are theoretical reasons to improve defenses and require more sophisticated capabilities for operational success, can it be done, either in specific situations or more generally? It is worth dividing this question into two parts: activities a state can undertake to increase what is required for operational success against its networks and those a state can perform to raise the bar generally.

It is obvious what states can do to better protect their own networks. Some cybersecurity practices, such as code auditing, patch application, regular maintenance, network security monitoring and the like can dramatically improve a network's security. These sorts of activities should be part of a baseline for any important computer system. There is no silver bullet product or idea that will solve computer security, but a commitment to the ongoing process of strengthening network security pays strong dividends. All states, but especially those that have valuable information or critical components connected to the internet, should improve their performance in these areas. A significant number of the threats states face do not rely on sophisticated capabilities and would be thwarted by improved security. ^[27] Such improvements enable states to focus on the more sophisticated threats that truly do matter, and not on the noise of less sophisticated actors.

There are reasons states have been slow to make progress in this area, however. Old legacy systems often contain critical data or perform important functions, but were not built with security in mind. Bureaucratic battles can complicate the process of updating hardware, software, and procedures. Users often need to be trained or retrained, and old habits sometimes die hard. Budget squabbles can slow or thwart major efforts to make wholesale improvements. ^[28] But an opportunity is in sight: if states can manage to get better at doing the basics, they can simplify the problem of cybersecurity and reduce the danger less sophisticated actors pose.

It is more complicated and hotly debated to consider what states might do to shift the balance more broadly to defenders. Some might argue that it is not sensible for sophisticated states to pursue this goal; if they are able to secure their own important computer networks, then that will be enough. Others,

though, might accept offense-defense theory's conclusion that a defense-dominant system is more stable, might believe in strongly prioritizing defense in certain types of software, or might conclude that states will have to take some action with a general impact in order to secure systems of importance to them.

This debate often crystallizes very narrowly around the matter of software vulnerabilities that sometimes enable intrusions. A sophisticated state that finds a vulnerability need not use it for such purposes. Instead, they can report it to the software vendor for remediation and patching. Doing so will likely involve giving up the possibility for action—the state foregoes its capacity to exploit the vulnerability against some targets—but makes it harder for other states to find and exploit the vulnerability. Even if a state preserves a small number of hard-to-exploit vulnerabilities for its own sophisticated operations, reporting the vast majority of vulnerabilities would perhaps improve computer security in the affected software. In so doing, the logic goes, reporting vulnerabilities shifts the advantage to the defense and increases stability. It is for this reason that major government review groups, civil society advocates, and—to some degree—government officials, advocate for a strong disclosure program. ^[29]

This view has its critics. Some cast doubt on whether vulnerability disclosure actually increases security, contending that states are unlikely to find and exploit the same vulnerabilities as other states. Some others point out that vulnerabilities are usually only found through significant work; if intelligence agencies are merely going to turn the vulnerability over for remediation, they do not have the incentive to do this work. Still others reject the notion that sophisticated states should constrain their own action at all. They argue that instead, they should press their advantage as much as they can. ^[30]

As spirited as both sides in the debate are, there are not enough public data to resolve the matter. It is hard to know the number of times that vulnerabilities are discovered independently by different actors—though quotes from former White House officials and some private sector surveys indicate that it does regularly happen. ^[31] It is likewise hard to recognize from afar all of the confounding factors in play in a decision to disclose or exploit, such as whether the affected software is disproportionately used in certain locations or whether it is in particularly important systems. ^[32] Understanding the incentive structure of those in government who find vulnerabilities can also be similarly difficult.

The goal here is simply to link the policy questions to more abstract ideas about sophistication. Whatever default position a state chooses for vulnerability disclosure and similar questions, its policy should have a firm conceptual foundation. Especially for a state with significant resources, policymakers have incentives to develop a consistent approach that recognizes their own capacity for sophistication, decides when to develop and deploy more specialized capabilities, and considers how it is possible to minimize the dangers posed by less capable actors. When it comes to sophistication, integrating theoretical nuance and practical considerations can shed light.

Conclusion: The Value and Limits of Sophistication

The idea of a credible spectrum of sophistication is analytically alluring. The sort of technical and operational paradigm outlined in this paper can yield a mechanism for practical comparison between a wide range of cyber threats. It can provide insight into the choices intruders make, the tradeoffs between cost, effectiveness, and timeliness they must balance, and the barriers to entry for some kinds of operations. A nuanced notion of sophistication can help researchers, defenders, and observers better focus their attention and spot significant details. At a minimum, it guides the overall assessment so that basic capabilities are not misunderstood or mislabeled, especially in the production or consumption of media reporting.

For network defenders, a sharper understanding of the sophistication of their potential adversaries' capabilities enables them to better conceptualize and prepare for threats. They will better understand the tradeoffs in specialization that their adversaries make. For many entities, an analysis of sophistication will conclude that their adversaries are perhaps not as advanced as they once feared, and that basic improvements in their defensive posture would make a meaningful difference in preventing intrusions. In short, once the legend of sophistication gets replaced with reality-based threat assessment, network defense becomes more practical, more focused, and probably more successful. This sort of threat modeling has long been around but is too frequently ignored. It should be considered a key part of network defense.

A more nuanced conception of sophistication has theoretical relevance, too. Those who wish to apply offense-defense theory to cyber operations will have to reckon with the concept. Much work remains to be done in order for this theory to be useful in the digital domain. Bedrock ideas are similarly improved by an understanding of what sophistication looks like, what it enables, and what differences in sophistication mean for the international system more broadly. Just as in conventional security studies, different capabilities enable different possibilities. Detailed examination of new capabilities and their strategic effects enhanced much of the study of nuclear weapons, where tradeoffs due to resource-constraints also had to be made. As the study of the cyber operations develops, a similar technically-sound foundation will become even more of a necessity. A refined framework for assessing variations of sophistication is important in this effort.

At the union of the practical and the theoretical is national policy. Here too a better understanding of sophistication has value. States with access to intelligence may be better able to resolve some challenging questions, such as those related to the capabilities of other actors. They may be able to get a better grasp on what choices their adversaries have made about how to invest their resources. Governments certainly will have to tackle many of the questions directly related to sophistication. These include whether lesser actors face a lower barrier to entry in building up cyber capabilities, in what operational areas governments should invest in pursuit of sophistication, or whether more sophisticated

actors can raise the bar on what is required for operational success. These policy questions are likely to grow, not fade, in relevance; they certainly have begun to attract a great deal of public attention. ^[33]

This paper contends that these discussions require a rigorous approach. A technical and operational framework like the one outlined in the second section can provide a standardized method for evaluating the choices intruders make. Forensic analysis of intrusions, which has become quite popular and salient in recent years, can be better guided by questions of sophistication. Factors like speed, mistakes, and scope can also give an indication as to the capability and experience of intruders. In short, data already exist waiting to be analyzed via the lens of sophistication. There is good reason to think that more thorough analysis is doable and valuable.

As useful as a more nuanced understanding of sophistication is, it has some important limits for strategic analysis. Intruders have an incentive to be just as sophisticated as required for an operation, and not more. Every entity has budget constraints. Analysts should never think that an actor lacks sophistication just because its operators used publicly available tools or employed common techniques. As with other forms of observation, when examining sophistication it is important to remain skeptical and alert to the possibility of misdirection and incomplete information. This challenge is simply a part of the study of cyber operations.

Some of the wounds to rigorous analysis—and, conversely, the fueling of the sophistication legend—are self-inflicted and self-perpetuating. Too often, companies that suffer a breach will describe the intruders with strong but inaccurate claims of sophistication. Too frequently, media outlets eager for a story will hype threats beyond what is reasonable or will elide technically-important distinctions between classes of operations. This sort of presentation waters down the concept of sophistication and dulls its practical and theoretical usefulness. At worst, it makes defending against cyber attacks seem like an exercise in futility. Scholars and practitioners, including media members, should take care to avoid such a crude approach. Both groups would benefit from an approach with more rigor, the beginnings of which were outlined here. The world of cyber operations is simply more complex, rife with both possible opportunities and confusion, than the legend of sophistication lets on.

Bibliography

Abdollah, Tami, 'Obama Seeks Cybersecurity Boost to Replace 'Ancient' Tech', Associated Press, 9 February 2016, <http://www.pbs.org/newshour/rundown/obama-seeks-cybersecurity-boost-to-replace-ancient-tech/> 

———, 'US Official: Hackers Targeted Election Systems of 20 States', Associated Press, 30 September 2016, <https://www.abcnews.com/66f67fb26d844f28bd18a522811bdd18/US-official-Hackers-targeted-election->

<https://www.apnews.com/60161b30d0474120b1ba32201bda10/US-Official-Hackers-targeted-election-systems-of-20-states> [↗](#)

Aitel, David, 'Useful Fundamental Metrics for Cyber Power', CyberSecPolitics, 22 June 2016, <https://cybersecpolitics.blogspot.com/2016/06/useful-fundamental-metrics-for-cyber.html> [↗](#)

Aitel, David, and Matt Tait, 'Everything You Know About the Vulnerability Equities Process Is Wrong', Lawfare, 18 August 2016, <https://lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong> [↗](#)

'APT1', Mandiant, 18 February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [↗](#)

Biddle, Sam, 'The NSA Leak Is Real, Snowden Documents Confirm', The Intercept, 19 August 2016, <https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/> [↗](#)

Brenner, Joel, *Glass Houses*. New York: Penguin, 2014.

Broad, William, John Markoff, and David Sanger, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', New York Times, 15 January 2011, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all> [↗](#)

Buchanan, Ben, *The Cybersecurity Dilemma*. New York: Oxford University Press, 2017.

———, 'The Life Cycles of Cyber Threats'. *Survival* 58, no. 1 (2016).


Burgess, Matt, 'TalkTalk Hack: Fourth Arrest and Government Inquiry Launched', Wired, 4 November 2015, <http://www.wired.co.uk/article/talktalk-hack-fourth-arrest-police-london-norwich> [↗](#)

Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz, 'The Diamond Model of Intrusion Analysis', Defense Technical Information Center, 5 July 2013, <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA586960> [↗](#)


Clarke, Richard, and Robert Knake, *Cyberwar*. New York: HarperCollins, 2010.

Clarke, Richard, and Robert Knake, *Cyberwar*. New York: HarperCollins, 2010.

Clarke, Richard, Michael Morell, Geoffrey Stone, Cass Sunstein, and Peter Swire, 'Liberty and Security in a Changing World', The President's Review Group on Intelligence and Communications Technologies, 12 December 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf 


Daniel, Michael, 'Heartbleed: Understanding When We Disclose Cyber Vulnerabilities', The White House Blog, 28 April 2014, <http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities> 


Elgin, Ben, and Michael Riley, 'Now at the Sands Casino: An Iranian Hacker in Every Server', Bloomberg, 11 December 2014, <http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas> 

'Equation Group: Questions and Answers', Kaspersky Lab, February 2015, http://cdn.securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf 

Fisher, Phineas, 'Hack Back! A DIY Guide', PasteBin, 17 April 2016, <http://pastebin.com/OSNSvyjJ> 


Friedersdorf, Conor, 'Encryption Backdoors Are Opposed by Former Government Officials', The Atlantic, 30 July 2015, http://www.theatlantic.com/politics/archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848/?utm_source=SFTwitter 

Goodin, Dan, 'New Smoking Gun Further Ties NSA to Omnipotent "Equation Group" Hackers', ArsTechnica, 11 March 2015, <http://arstechnica.com/security/2015/03/new-smoking-gun-further-ties-nsa-to-omnipotent-equation-group-hackers/> 

Greenwald, Judy, 'Insurer Cites Cyber Policy Exclusion to Dispute Data Breach Settlement', Business Insurance, 15 May 2015, <http://www.businessinsurance.com/article/20150515/NEWS06/150519893> 


Healey, Jason, "A Non-State Strategy for Saving Cyberspace," Atlantic Council, January 2017,


http://www.atlanticcouncil.org/images/publications/AC_StrategyPapers_No8_Saving_Cyberspace_WEB.pdf 

Hern, Alex, 'TalkTalk Hit with Record £400k Fine over Cyber-Attack', The Guardian, 5 October 2016, <https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack> 


Isikoff, Michael, 'FBI Says Foreign Hackers Penetrated State Election Systems', Yahoo News, 29 August 2016, <https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html> 


Jervis, Robert, 'Cooperation under the Security Dilemma'. *World Politics* 30, no. 2 (1978): 167-214.

Johnston, Chris, 'TalkTalk Customer Data at Risk after Cyber-Attack on Company Website', The Guardian, 22 October 2015, <https://www.theguardian.com/business/2015/oct/22/talktalk-customer-data-hackers-website-credit-card-details-attack> 

Kagan, Frederick W., and Tommy Stiansen, 'The Growing Cyberthreat from Iran', American Enterprise Institute/Norse, April 2015, <https://www.aei.org/wp-content/uploads/2015/04/Growing-Cyberthreat-From-Iran-final.pdf> 

Menn, Joseph, 'Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback', Reuters, 10 May 2013, <http://uk.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510> 


Mimoso, Michael, 'Inside nls_933w.dll, the Equation APT Persistence Module', ThreatPost, 17 February 2015, https://threatpost.com/inside-nls_933w-dll-the-equation-apt-persistence-module/111128 

Nakashima, Ellen, and Andrea Peterson, 'Obama Faces Growing Momentum to Support Widespread Encryption', Washington Post, 16 September 2015, https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html 


Ozment, Andy. "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting." In *The Workshop on Economics and Information Security*. Cambridge, MA, 2005.


Perlroth, Nicole, 'Unable to Crack Computer Virus, Security Firm Seeks Help', New York Times, 14 August 2012, <http://bits.blogs.nytimes.com/2012/08/14/unable-to-crack-computer-virus-security-researchers-issue-cry-for-help/> 

'ProjectSauron: Top Level Cyber-Espionage Platform Covertly Extracts Encrypted Government Comms', Kaspersky Lab, 8 August 2016, <https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/> 

Rid, Thomas, and Ben Buchanan, 'Attributing Cyber Attacks'. *Journal of Strategic Studies* 39, no. 1 (2015), <http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382> 

Robinson, Tony, 'Cat and Mouse: The Effects of Threat Research on Nation-State Actors', Rally Security, 19 August 2016, <http://rallysecurity.com/cat-and-mouse-the-effects-of-threat-research-on-nation-state-actors/> 

Schwartz, Ari, and Robert Knake, 'Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process', Belfer Center for Science and International Affairs, 17 June 2016, <http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf> 

'Security Breach Notification Laws', National Conference of State Legislatures, 4 January 2016, <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> 


'Taia Global Linguists Establish Nationality of Sony Hackers as Likely Russian, Not Korean', Taia Global, 8 January 2015, <https://taia.global/2014/12/taia-global-linguists-establish-nationality-of-sony-hackers-as-russian-not-korean/> 

'TalkTalk Cyber-Attack: Website Hit by 'Significant' Breach'. BBC News. 23 October 2015.

<http://www.bbc.com/news/uk-34611857> 

Zetter, Kim, *Countdown to Zero Day*. New York: Crown, 2014.

———, ‘How the NSA’s Firmware Hacking Works and Why It’s So Unsettling’, *Wired*, 22 February 2015, <http://www.wired.com/2015/02/nsa-firmware-hacking/> 

———, ‘Suite of Sophisticated Nation-State Attack Tools Found with Connection to Stuxnet’, *Wired*, 16 February 2015, <http://www.wired.com/2015/02/kaspersky-discovers-equation-group/> 

Notes

[1] ‘Equation Group: Questions and Answers’, Kaspersky Lab, February 2015, 3.

[2] Dan Goodin, ‘New Smoking Gun Further Ties NSA to Omnipotent “Equation Group” Hackers’, *ArsTechnica*, 11 March 2015; Kim Zetter, ‘Suite of Sophisticated Nation-State Attack Tools Found with Connection to Stuxnet’, *Wired*, 16 February 2015; Sam Biddle, ‘The NSA Leak Is Real, Snowden Documents Confirm’, *The Intercept*, 19 August 2016.

[3] ‘TalkTalk Cyber-Attack: Website Hit by ‘Significant’ Breach’, *BBC News*, 23 October; Chris Johnston, ‘TalkTalk Customer Data at Risk after Cyber-Attack on Company Website’, *The Guardian*, 22 October 2015; Matt Burgess, ‘TalkTalk Hack: Fourth Arrest and Government Inquiry Launched’, *Wired*, 4 November 2015.

[4] For an overview, see ‘Security Breach Notification Laws’, *National Conference of State Legislatures*, 4 January 2016.

[5] Tony Robinson, ‘Cat and Mouse: The Effects of Threat Research on Nation-State Actors’, *Rally Security*,

19 August 2016. For an example of a cyber insurance dispute, see Judy Greenwald, ‘Insurer Cites Cyber Policy Exclusion to Dispute Data Breach Settlement’, Business Insurance, 15 May 2015.

[6] ‘APT1’, Mandiant, 18 February 2013.

[7] The now-defunct cybersecurity firm Norse gained a reputation for overhyping threats. For example, see Frederick W. Kagan and Tommy Stiansen, ‘The Growing Cyberthreat from Iran’, American Enterprise Institute/Norse, April 2015.

[8] ‘Taia Global Linguists Establish Nationality of Sony Hackers as Likely Russian, Not Korean’, Taia Global, 8 January 2015.

[9] Kagan and Stiansen, ‘The Growing Cyberthreat from Iran’, American Enterprise Institute/Norse.

[10] David Aitel, ‘Useful Fundamental Metrics for Cyber Power’, CyberSecPolitics, 22 June 2016.

[11] Properly speaking, this is the Basic Input/Output System, but it is rarely referred to as such.

[12] For greater development of this idea, see Ben Buchanan, *The Cybersecurity Dilemma* (New York: Oxford University Press, 2017).

[13] Ben Elgin and Michael Riley, ‘Now at the Sands Casino: An Iranian Hacker in Every Server’, Bloomberg, 11 December 2014.

[14] Michael Mimoso, ‘Inside nls_933w.dll, the Equation APT Persistence Module’, ThreatPost, 17 February 2015.

[15]

— **‘ProjectSauron: Top Level Cyber-Espionage Platform Covertly Extracts Encrypted Government Comms’, Kaspersky Lab, 8 August 2016.**

[16] — **Alex Hern, ‘TalkTalk Hit with Record £400k Fine over Cyber-Attack’, The Guardian, 5 October 2016.**

[17] — **Phineas Fisher, ‘Hack Back! A DIY Guide’, PasteBin, 17 April 2016.**

[18] — **For more on attribution see Thomas and Ben Buchanan, ‘Attributing Cyber Attacks’, *Journal of Strategic Studies* 39, no. 1 (2015); Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, ‘The Diamond Model of Intrusion Analysis’, Defense Technical Information Center, 5 July 2013.**

[19] — **For more on Stuxnet’s testing, see William Broad, John Markoff, and David Sanger, ‘Israeli Test on Worm Called Crucial in Iran Nuclear Delay’, New York Times, 15 January 2011.. For more on later efforts at obfuscation and operational security, see Nicole Perlroth, ‘Unable to Crack Computer Virus, Security Firm Seeks Help’, New York Times, 14 August 2012; Kim Zetter, *Countdown to Zero Day* (New York: Crown, 2014).**

[20] — **On the other hand, sometimes timing and budgets concerns will make perfect conservation of sophistication difficult, as states sometimes have to use whatever is readily available, even if it is overkill. But it is tougher to judge when this happens using public domain evidence.**

[21] — **Mimoso, ‘Inside nls_933w.dll, the Equation APT Persistence Module’, ThreatPost; Kim Zetter, ‘How the NSA’s Firmware Hacking Works and Why It’s So Unsettling’, Wired, 22 February 2015.**

[22] — **For book-length articulations of this view, see Richard Clarke and Robert Knake, *Cyberwar* (New York: HarperCollins, 2010); Joel Brenner, *Glass Houses* (New York: Penguin, 2014).**

[23] — **Some capabilities will diffuse between actors, but certain categories of sophisticated capabilities are less likely to. For more see Ben Buchanan, ‘The Life Cycles of Cyber Threats’, *Survival* 58, no. 1 (2016).**

[24] Jason Healey, “A Non-State Strategy for Saving Cyberspace,” Atlantic Council, January 2017.”

[25] For a seminal article, see Robert Jervis, ‘Cooperation under the Security Dilemma’, *World Politics* 30, no. 2 (1978).

[26] For a broader discussion of this point, see Buchanan, *The Cybersecurity Dilemma*, Ch 5.

[27] There are many examples. Recent ones include the breach of voter registration systems enabled by SQL injection, a very basic vulnerability. Michael Isikoff, ‘FBI Says Foreign Hackers Penetrated State Election Systems’, Yahoo News, 29 August 2016. Tami Abdollah, ‘US Official: Hackers Targeted Election Systems of 20 States’, Associated Press, 30 September 2016.

[28] Tami Abdollah, ‘Obama Seeks Cybersecurity Boost to Replace ‘Ancient’ Tech’, Associated Press, 9 February 2016.

[29] For two prominent examples, see Ari Schwartz and Robert Knake, ‘Government’s Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process’, Belfer Center for Science and International Affairs, 17 June 2016; Richard Clarke et al., ‘Liberty and Security in a Changing World’, The President’s Review Group on Intelligence and Communications Technologies, 12 December 2013.

[30] For one perspective that makes many of these arguments, see David Aitel and Matt Tait, ‘Everything You Know About the Vulnerability Equities Process Is Wrong’, Lawfare, 18 August 2016.

[31] Andy Ozment, “The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting,” in *The Workshop on Economics and Information Security* (Cambridge, MA, 2005); Joseph Menn, ‘Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback’, Reuters, 10 May 2013.

[32] For an example of some of the criteria that are acknowledged to go into this decision, see Michael Daniel, ‘Heartbleed: Understanding When We Disclose Cyber Vulnerabilities’, The White House Blog, 28 April 2014.

[33] In addition to the discussion about vulnerability disclosure, encryption and the related security questions attracted major attention in 2015 and 2016. For example, see Conor Friedersdorf, ‘Encryption Backdoors Are Opposed by Former Government Officials’, The Atlantic, 30 July 2015; Ellen Nakashima and Andrea Peterson, ‘Obama Faces Growing Momentum to Support Widespread Encryption’, Washington Post, 16 September 2015.

RECOMMENDED CITATION

Buchanan, Ben . “The Legend of Sophistication in Cyber Operations.” *Cyber Security Project*, Belfer Center, January 2017

AUTHOR

Ben Buchanan

Prepared Testimony: House Oversight Committee

More From This Expert Nonlethal Weapons and Cyber Capabilities

79 John F. Kennedy Street,
Cambridge, MA 02138