A HOOVER INSTITUTION ESSAY

Nobody But Us

THE RISE AND FALL OF THE GOLDEN AGE OF SIGNALS INTELLIGENCE

BEN BUCHANAN

Aegis Series Paper No. 1708

Introduction

The United States' National Cryptologic Museum in Fort Meade, Maryland, displays versions of two important encryption machines. The first is the Enigma machine, the most famous cryptographic apparatus ever built. The second machine, less well known, is called SIGABA. These devices are similar in certain important respects. Each employs an electromechanical rotor-based design. Each was used during World War II; the Nazis deployed Enigma while US forces relied on SIGABA. It is no exaggeration to say that, during the conflict, these machines protected—or tried to protect—some of the most important messages in the world.

Both sides treated the machines as closely guarded secrets. The United States took enormous steps to protect SIGABA, requiring that it only be deployed to areas where American forces could guard it and instructing these forces to destroy the machines before they could be captured.[1] American cryptologists feared what could happen if the enemy gained access to SIGABA and reverse engineered it. On the other hand, the Allies achieved an enormous success when they captured an Enigma machine. Acquiring the physical device was one of the many factors that enabled the Allies to eventually understand its workings and decrypt the messages it protected.[2]

These encryption devices are more than just historical artifacts. They represent perhaps the purest form of signals intelligence work. One machine represents the challenge of breaking an enemy's code, while the other represents the imperative to secure friendly communications. Which machine represents which, of course, depends on allegiance.

These two missions—decrypt enemy communications and protect one's own—have not been in direct conflict for most of the history of signals intelligence. Indeed, the Allies' success in cracking Enigma while protecting SIGABA demonstrates as much.

I would like to thank Jack Goldsmith, Herb Lin, Gabriella Roncone, Paul Rosenzweig, Michael Sulmeyer, and Ben Wittes for comments on an earlier draft of this paper. All errors remain mine alone.

But while nations still use proprietary technology and codes to securely transmit their secrets, in important respects the signals intelligence environment is now fundamentally different.

Today, American adversaries rely on many of the same technologies to transmit and protect their secrets as the United States does for its own sensitive information. Governments all over the world run the same operating systems. Terrorists and ordinary citizens use the same models of phones. Core Internet routers carry everyone's communications while common encryption algorithms try to safeguard those messages. This makes the signals intelligence mission, once bifurcated into offense and defense, murkier and more complex. Often, the means of secret stealing are in tension with the means of secret securing.

As a highly digitized society, the United States feels this paradox acutely. For several decades, its approach to resolving the tension can be characterized as Nobody But Us (more commonly shortened to NOBUS). Sometimes the National Security Agency (NSA) explicitly uses this terminology, but often the idea is more implicit and more emergent. Different parts of the agency handle a wide range of tasks, including acquiring communications, hacking targets, and breaking encryption. The NOBUS approach is relevant to all of these missions.

The premise of the NOBUS approach is simple: when there is tension between offense and defense, the United States aspires to secure communications against all forms of signals intelligence collection—except those forms of interception that are so complex, hard, or inaccessible that only the United States uses them. When the United States develops and deploys its special and esoteric collection capabilities and blocks simpler means of collection, it can, in theory, protect its own communications and secrets but still acquire those of others. NOBUS does not mean that adversaries do not know much of American capabilities, though they frequently do not. It simply means they cannot match them and, in many cases, struggle to thwart them.

Unique American advantages enable the NOBUS approach. Some of these advantages are geographical, since the United States has access to important cables carrying the world's communications. Sometimes they are commercial, as American companies store valuable data and are subject to American legal demands. Sometimes they are technical or are the result of enormous investment: the NSA's combination of mathematical skill and supercomputing power is an example of this. Other times they

involve the discovery of specific knowledge, such as a software vulnerability that an adversary is unlikely to find. All told, these advantages create a capability gap between the United States and the rest of the world. NOBUS capabilities exist in this gap.

For a while, the NOBUS approach worked well. It in part enabled what the NSA has called the golden age of signals intelligence.[3] During this period, many American adversaries knew enough to communicate with digital technologies but not enough to try to secure them. In the cases where adversaries did deploy better tradecraft, the United States used its technological advantages to great effect, in line with the NOBUS approach. While there were still real technical challenges and tough policy judgment calls—for example, how does one determine that another nation is not capable of developing the same interception method?—the NOBUS approach appeared to be an overall success.

This paper argues that the era characterized by the NOBUS approach is under serious stress and is quickly coming to an end. Adversaries are increasingly sophisticated. Technology providers now deploy ever-improving encryption by default. Demands for access stretch beyond the intelligence community to include law enforcement. As a result, reliance on NOBUS capabilities is no longer as effective as it once was. This has serious consequences for the United States and requires careful study and shrewd policy making.

The paper proceeds in three sections. The first examines the NOBUS approach in more detail. It outlines the ways in which the United States can and does exploit structural or asymmetric advantages in capability or access to enable NOBUS methods. The second section examines how current trends make NOBUS solutions harder to find and use. The third and concluding section articulates some ideas for a potential path forward, though it acknowledges there is no easy answer.

The Problem NOBUS Tries to Solve

The NOBUS approach attempts to resolve a fundamental tension that often exists between offense and defense: carrying out one mission can diminish the other. This is true at a variety of levels. As former NSA security scientist David Aitel wrote, "The problem is a fractal. The U.S. government cannot agree on any one cyber issue, but if you drill down, neither can the Department of Defense, and if you go deeper, the NSA cannot agree with itself on these issues. No matter how far down the chain you go, there are competing initiatives."[4]

This tension is acute in an era in which friendly and adversarial users rely on common software platforms, security mechanisms, and providers to transmit communication. The possible areas of overlap are nearly limitless, and examples can be easily imagined. Perhaps an adversary's military uses Windows, but so does a large percentage of the US government. This means that if the United States wants to leave Windows vulnerable to some kinds of hacking so it can target the adversary, it runs the risk that others will use the same vulnerabilities to target the United States.

Or maybe an organized crime group with ties to foreign intelligence agencies uses the Signal encryption protocol, but so do the billion people who use the messaging program WhatsApp. The United States will find it hard to undermine the Signal cryptography just when the organized crime group uses it, but not when others do. Or if a terrorist suspect has a Gmail account, the United States must find a way to gather only the communications of the suspect, and not those of innocent users. Everyone's data goes over the same fiber-optic cables, meaning that signals intelligence agencies need to determine which data they collect and store.

To be sure, there are signals intelligence activities without this tension—intercepting and decoding the radio signals sent by a foreign military using its own technology and encryption, for example—but those represent a smaller percentage of the whole now than a few decades ago. In an era of convergence, NOBUS capabilities are increasingly important tools for signals intelligence agencies.

This section outlines how the United States has historically been well positioned to develop and deploy NOBUS signals intelligence capabilities. It focuses on NOBUS capabilities in four areas of analysis: encryption, software vulnerabilities, bulk collection from telecommunications providers, and legal demands to companies with meaningful data. In each of these areas, the United States has had unique or near-unique capacity to achieve the NOBUS standard.

Encryption

The idea behind encryption is simple, even if the math rarely is. Cryptography enables two parties to encrypt a message such that only the intended recipient can decrypt it. In a properly implemented cryptographic system, even if eavesdroppers intercept the message in its entirety, they cannot understand it. Using a technology known as public key encryption, it is possible to securely encrypt and transmit messages without any prearranged signals or codebooks. This is in contrast to both Enigma and

SIGABA, which depended on the distribution of codebooks with predetermined keys to accompany each of the machines. These books, if captured, would have enabled the decryption of messages.

Encryption poses an immediate problem for signals intelligence agencies. If the messages they intercept are encrypted and thus cannot be deciphered, then the content of these intercepted messages is of comparatively limited intelligence value. On the other hand, if the messages an agency or the citizens of the agency's nation transmit do not have secure encryption, adversaries can easily understand them if intercepted.

The NOBUS idea offers a tantalizing solution. After a series of failed public attempts to mandate a NOBUS-like encryption mechanism in the 1990s, the NSA appears to have pursued it in secret. Around 2000, the agency began a highly classified effort to undermine encryption; the code name references a bloody Civil War battle and suggests the challenges of attacking systems used by one's own citizens.[5] The first NOBUS method as applied to encryption is to insert a so-called back door into the encryption algorithm. Roughly speaking, this back door reduces the security of the system, usually enabling an eavesdropper with knowledge of the back door to decrypt messages. Those who do not know the details of the back door, however, are no more empowered to decrypt, provided that the back door remains hidden. A prominent example is the back door the NSA placed in a pseudorandom number generator—a key part of encryption implementations—known as Dual_EC_DRBG. While the math behind the back door is beyond the scope of this paper, it enabled those who knew of it to break encryption that relied on Dual_EC_DRBG.[6]

Structural advantages meant that this back door was a NOBUS solution. The American government enjoys disproportionate, perhaps even unique, influence through its cryptographic validation program, which verifies encryption algorithms as secure. The United States National Institute for Standards and Technologies, which is not part of the intelligence community, is involved in putting forth encryption algorithms that can meet these standards. The NSA was able to influence the American bureaucratic process so that it was the "sole editor" of the Dual_EC_DRBG specification and could insert the back door of which only it knew.[7]

In effect, by having the government certify algorithms known to be insecure as safe for use, the NSA leveraged the American government's exceptional credibility

to encourage corporations and other entities to deploy exploitable encryption. A nation like Russia or Iran would almost certainly not enjoy the same level of trust in its government-supported encryption. In addition, it is reported that the NSA further incentivized the use of the weak encryption component by secretly paying an American computer and network security company, RSA, $10 million to rely on the flawed pseudorandom number generator in some of its products.[8]

A second NOBUS approach to defeating encryption is to find weaknesses in the encryption implementations that can be exploited at scale. One theorized example of this is a weakness in a mechanism known as the Diffie-Hellman key exchange, which underpins a substantial portion of modern encryption implementations. The concept of Diffie-Hellman requires that the sender and receiver agree on using a large prime number with a particular mathematical form. In practice, many of the world's Diffie-Hellman implementations reuse the same specific prime number. This reuse could enable an organization with a massive amount of computing power to crack one of the widely used prime numbers and overcome the encryption.

One estimate is that an investment of several hundred million dollars would enable the construction of a supercomputer capable of cracking one Diffie-Hellman prime per year. Doing this for even one prime would enable the decryption of two-thirds of the virtual private networks in the world. Managing to do it for another would enable the decryption of around one-fifth of all the encryption commonly used to secure web traffic, known as https.[9] The resources and skill required to build such computing power would presumably render this kind of compromise of Diffie-Hellman a NOBUS capability, though the supercomputing power of foreign intelligence agencies is hidden from public view.

It is not known for certain that the NSA employed or employs such methods against Diffie-Hellman in particular. The price tag of the cracking effort described here is certainly within reach, as the agency's budget is more than $10 billion, with more than $250 million dedicated each year to the encryption-breaking BULLRUN program.[10] In its so-called black budget request in 2013, the NSA placed a priority on "investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit internet traffic."[11] An internal file indicates that there is a compartment of highly classified information that covers the NSA efforts to "exploit SIGINT targets by attacking the hard mathematical problems underlying public key cryptography" (Diffie-Hellman is one of the most prominent examples of a public

key-based system).[12] Other documents indicate that the agency has significant passive large-scale decryption capabilities and that it pursues the collection of information consistent with cracking Diffie-Hellman. All told, two of the authors of a major paper on Diffie-Hellman security, Alex Halderman and Nadia Heninger, conclude that this kind of decryption effort "fits the known technical details about [the NSA's] large-scale decryption capabilities better than any competing explanation."[13] If their analysis is correct, this is likely the NOBUS approach at work.

Software Vulnerabilities

The famous cryptographer Adi Shamir introduced an idea so important that it has come to be known as Shamir's Law: cryptography is usually bypassed, not broken. That is, for all the capabilities of signals intelligence agencies to crack encryption protocols or implementations, they often find it easier to circumvent them. In short, gaining remote access to the devices that transmit messages enables easier interception. Such access can also enable the acquisition of key documents, further lateral movement within a target network, and aid the development and deployment of cyberattacks.[14]

This access is often gained using malicious code. Frequently, social engineering such as spear-phishing enables the deployment of this malicious code or obviates the need for it, but not always. Sometimes, cyber operators will deploy code, known as an exploit, that takes advantage of a vulnerability in software run by the target. Typically, this will enable the hacker to do something unauthorized, such as run additional malicious code. The additional code can give the hacker a large degree of remote access to the computer, including the ability to record what is typed on the keyboard and seen on the screen, the ability to develop a persistent presence on the computer that is hard to remove, and the ability to spread to other computers on the network.

The most significant of these exploits, known as "zero day exploits," are unknown to software vendors before their use. There is thus no security fix that addresses these vulnerabilities, although there are some security products that try to spot signs of post-exploitation malicious activity. In short, the owners of a computer targeted with a zero day exploit, even if they follow solid security procedures and keep their systems up to date, will have a difficult time repelling an intrusion.[15] As such, developing and using zero day exploits is an essential part of maintaining an advanced signals intelligence capability. But doing so is a significant challenge, with only a comparatively small number discovered each year.

The United States actively looks for zero day exploits to fuel its cyber operations. In addition to a secret program in which it purchases zero days from vendors,[16] the US intelligence community seeks to find its own. As one part of this effort, it has turned its vast signals intelligence capabilities toward intercepting Windows crash reports sent over the Internet, in the hope that a software failure could reveal an exploitable vulnerability.[17] All of this is to significant effect: the United States is able to use what it finds to enable a wide range of potent operations. For example, Stuxnet, the malicious code that attacked the Iranian nuclear program, deployed at least five zero days of various types—an unprecedented number for a single operation.[18]

When the United States discovers or buys a zero day, it has two choices: it can either use the newly discovered vulnerability by writing malicious code that exploits the weakness or it can notify the vendor of the affected software so that the problem can be fixed in a security update. The first approach can yield intelligence gains and can sometimes even enable significant attacks, as in the Stuxnet case. It can also leave computers, including American computers, at risk, however. If another sophisticated adversary discovers or buys the same vulnerability, it can use it in its own operations.

The second approach—disclosing the zero day vulnerability to the appropriate software vendor to fix it—is an attempt to promote general cybersecurity. The benefits of this course of action depend on vendors producing security patches and users applying them. Publicly disclosing the vulnerability might also increase trust in the United States as an actor advancing collective interests, which might make diplomatic engagements easier. At the same time, disclosing the vulnerability makes it somewhat harder to obtain intelligence because it partially deprives the United States of the ability to exploit the vulnerability. The potential to exploit it does not diminish entirely, however. If the likely targets of American operations fail to keep their systems up to date with software patches and security software—a failure which is more likely with less sophisticated actors—then the United States will still be able to use the exploit against them.

A statement from the Obama White House on software vulnerabilities indicated that the United States, as a general rule, tries to focus on exploiting vulnerabilities used in its targets' software and would try to report vulnerabilities in American software.[19] But, inevitably, there is overlap. The NOBUS approach can provide a way forward. Former NSA director Michael Hayden indicated that the NOBUS idea was a specific criterion in

determining which of the vulnerabilities in widely used software to exploit and which to report. He said:

> You look at a vulnerability through a different lens if even with the [knowledge of the] vulnerability it requires substantial computational power or substantial other attributes and you have to make the judgment who else can do this? If there's a vulnerability here that weakens encryption but you still need four acres of Cray [super]computers in the basement in order to work it you kind of think "NOBUS" and that's a vulnerability we are not ethically or legally compelled to try to patch—it's one that ethically and legally we could try to exploit in order to keep Americans safe from others.[20]

Hayden's example acknowledges the possibility of NSA using its unique computational power to exploit vulnerabilities in encryption, as suggested above. More broadly, he alludes to the possibility that the NSA will find software vulnerabilities that, for a variety of reasons, the agency thinks it alone will discover or can exploit. If these truly are NOBUS capabilities, then the NSA can do so with the confidence that others will not be able to do the same.

Bulk Collection from Telecommunications Providers

To a large degree, modern signals intelligence runs on data. The United States, in partnership with the United Kingdom, Canada, Australia, and New Zealand in the so-called Five Eyes alliance, has done an exceptional job of developing a broad array of sources from which it can collect data in bulk. Bulk data collection enables a wide range of analysis, including the discovery of new targets and the observation of broader trends. There are few better forms of bulk collection than tapping the fiber-optic cables on which so much of the world's data travels.

By collecting data from fiber-optic cables, the NSA is able to access much of the Internet traffic entering, transiting, and exiting the United States (but, per apparent legal restrictions, the agency cannot collect all traffic that originates and terminates in the United States).[21] In addition, NSA documents indicate it has been "buying up real estate"[22] and tapping major Internet cables that serve other areas of interest.[23] These "includ[e] several that service the Russian market" and one that services "the Middle East, Europe, South America and Asia."[24] A program run by the Government Communications Headquarters (GCHQ), the British signals intelligence agency, uses

two hundred physical points of inspection to obtain data and supplement the NSA's efforts.[25] The program obtains data from the telecommunication providers BT, Verizon Business, Vodafone, Global Crossing, Level 3, Viatel, and Interoute, likely among others.

These partner companies may also enable access to cables operated by other companies at their landing sites, further increasing the reach of the program. This may have been what enabled the Five Eyes to access the fiber-optic cables used by some of the world's most important Internet companies, including Google and Yahoo. The cables link the technology firms' overseas datacenters; the secret access enabled the Five Eyes to perform additional broad collection.[26] All told, these fiber-optic collection efforts are part of a signals intelligence network that collects from "thousands of [internet] trunk groups connected worldwide."[27]

Scale is clearly a hallmark of all these collection programs. They are broad in nature, siphoning massive amounts of traffic for at least cursory (and often initially automated) analysis. In the case of GCHQ's program, for example, the tapped cables are capable of carrying up to ten gigabits per second, meaning that they "had the capacity, in theory, to deliver more than 21 petabytes a day—equivalent to sending all the information in all the books in the British Library 192 times every 24 hours."[28] The GCHQ program is designed to store all Internet data transiting the tapped wires for three days and to store all metadata for thirty days.[29] The program targeting Google and Yahoo is similarly scalable, targeting "high volume" cables and performing "full take" collection.[30] A massive amount of data passes through these private wires. In Yahoo's case, it included backup copies of millions of entire email accounts.[31]

This sort of collection appears to reach the NOBUS threshold. For geographic and historical reasons, the Five Eyes countries are positioned well to serve as the endpoints for some of the most significant data and phone connections in the world. This means that, even when citizens from their countries are not involved in the communication, it is likely that the traffic will be routed through the Five Eyes' geographic territory, enabling easier collection. For example, most of the trans-Atlantic cables with significant capacity run through Great Britain,[32] while cables running through the United States provide some of the key links between South America, Europe, and Asia.

For historical reasons relating to the pricing models of international phone networks, subsequently inherited by the Internet, it is often cheaper to route traffic and calls

through the United States even if it is physically farther. Most of the traffic from one South American country to another, for example, is routed through Miami.[33] All told, at one point about 90 percent of the world's Internet traffic crossed the United States, according to a leaked NSA estimate. It is unclear whether Edward Snowden's revelations or new trends in Internet use have changed this number.[34]

As a result, telecommunications companies in Five Eyes countries run many of the world's most important data hubs. In addition to geography, it is the relationships between Five Eyes governments and these companies that enable the NOBUS capability.[35] American companies are compelled by law to cooperate in certain ways with the US intelligence community and are collectively paid hundreds of millions of dollars per year as part of the United States' black budget for their assistance.[36] When asked about their fiber-optic cable tapping activities, British companies note that they also must comply with legal demands.[37] In addition, some telecommunications companies partnering with the United States and its allies go "well beyond" what is legally required.[38] For example, AT&T is praised in NSA documents for its "extreme willingness to help" route traffic in such a way that the NSA can collect it.[39] Whether that cooperation continues today is unclear.

While potential adversaries certainly have similar relationships with their telecommunication providers, the American (and other Five Eyes) firms are best positioned to be useful for collection purposes. Russian and Chinese telecommunications companies are substantially less well situated on the global network of cables. There is no evidence that they have been able to build out clandestine bulk collection capabilities from the Five Eyes telecommunications networks, though it is impossible to say for sure.

Where legal compellence is not an option and in the cases where the collection is outside the Five Eyes, the United States can draw on other unique relationships it enjoys. A program known as MYSTIC, for example, relies on the secret partnership between NSA and the Drug Enforcement Agency, which has eighty international offices and "close relationships with foreign government counterparts and vetted foreign partners."[40] The program leverages agreements with the local telecommunications companies for "legitimate commercial service," likely the provision of wiretaps for counternarcotic purposes. It covertly gives the NSA access to the foreign telephone networks; the Snowden documents note that "host countries are not aware of NSA's SIGINT collection [using these systems]."[41]

Legal Demands

The last three sections describe covert ways of gathering information of interest. There might be an easier approach: demand that the service provider with legitimate endpoint or data storage access to that information provide the desired information. A demand backed by legal power can make this process effective and scalable. Given the prominent role of American technology companies, the United States is best positioned to take this approach. This is one of the reasons that, when describing its collection activities internally, the NSA sometimes refers to its "home-field advantage" in cyberspace.[42]

To further its intelligence operations, the United States receives legally compelled cooperation from these companies, such as Microsoft, Yahoo, Google, Apple, Facebook, and more. A program known as PRISM enables the NSA to quickly receive information these companies have on a specific target, including emails, messages, images, videos, and Internet forum activity. The PRISM program is authorized under Section 702 of the FISA Amendments Act of 2008, which mandates that the collection must be in service of foreign intelligence purposes. This is an attempt—with widely debated effectiveness—to protect the privacy of US persons, even as it enables the collection of intelligence. Even American companies that do not participate in PRISM are subject to these Section 702 demands.[43]

It's reasonable to ask why the NSA uses the PRISM program when it already has the cable tapping system described above. NSA documents indicate that PRISM is a complement for this other collection, rather than a replacement, instructing the agency's analysts that they "should use both."[44] PRISM is uniquely valuable because it is difficult to predict how Internet traffic will move ahead of time, since routing depends so much on network conditions. Therefore, it is possible that the traffic of a target is routed in such a way that makes it more difficult for a signals intelligence agency to collect it using cable-based collection systems. PRISM also provides an opportunity to get data that the signals intelligence system may have missed the first time around.

Russia or China almost certainly cannot compel the same amount of disclosure of customer information from American companies. Therefore, once again, it is the United States' technological prominence coupled with its legal authorities that makes PRISM a NOBUS capability, and a valuable one at that. NSA documents claim that PRISM is the "[Signals Intelligence Activity Designator] used **most** in NSA reporting"[45] and is used in one out of seven reports overall.[46] Some of these reports made it to the

highest levels of government; PRISM-enabled collection was reportedly cited in the Presidential Daily Brief 1,477 times in 2012.[47] This is an intelligence advantage other nations are unlikely to match, since their companies do not store nearly as much data as the US tech sector does.

The Trouble with NOBUS

The NOBUS approach is powerful. Indeed, the last section outlined the structural advantages that enable NOBUS capabilities. But that edge is under serious threat. The danger arises from the combination of three trends, each of which poses a substantial risk: increasingly sophisticated adversaries, better and more widely deployed encryption, and growing overt demand for access to data. Taken together, these three factors portend trouble for NOBUS capabilities.

Increasingly Sophisticated Adversaries

The NOBUS approach, by definition, is about a capability gap between the United States and its adversaries. This gap serves American interests. Sometimes it is enabled by greater computing power and investment, sometimes by meaningful legal demands or covert relationships, sometimes by favorable geography or history, and sometimes by skill and resources. The gap narrows when adversaries catch up. To the extent that other nations, such as Russia and China, have increased their relative capabilities, they inevitably threaten the NOBUS approach.

Two examples, likely involving other nations, demonstrate this point. First, it is widely assumed that the NSA placed a back door in encryption software used by the Internet hardware company Juniper. Targeting Juniper is a canonical case of the need for a NOBUS capability. Some of the company's specific customers include AT&T, Verizon, NATO, and the US government, but also many overseas entities that would be plausible, if not likely, signals intelligence targets.[48]

The NSA likely placed this back door in 2008, when an unknown actor used unknown means to manipulate Juniper's code to make it susceptible to the Dual_EC_DRBG back door described earlier. The company denies doing this at NSA's direction.[49] However, three pieces of evidence suggest that the NSA would have reason to be involved: the agency's apparent compromise of the Dual_EC_DRBG standard; its secret efforts, described in internal documents, "to leverage sensitive, co-operative relationships with specific industry partners" to introduce weaknesses in American encryption;[50] and its

broad remit for collecting information. In so doing, the agency might have thought that it was using a NOBUS capability—one taking advantage, in secret, of a back door about which only the agency knew.

Four years later, another code change shattered the idea that the back door was still NOBUS. In 2012, an unknown actor manipulated the code further. This actor, almost certainly a new third party and quite likely a foreign intelligence service, manipulated the back door to enable its own decryption capability. It did so by swapping in its own numerical constants into the encryption implementation. The noted cryptographer Matthew Green analyzed the case and concluded, "The third party knowing these [constants] could now defeat Juniper's security. . . . Very little work was even required by the third party. They merely had to re-key the existing back door's lock—everything else was already pre-configured for their use."[51] A little less than two years after that, this third party or another actor also added a hard-coded password, enabling it to take complete control of the affected Juniper hardware. One analysis concluded that the case was "as terrible as it gets" in terms of security breach severity.[52]

This incident highlights the digital spy-versus-spy games between nations that are often just out of public view. It also demonstrates how sophisticated the best actors are.[53] If the commonly assumed narrative is correct—the NSA placed a back door in Juniper, but another nation found it and exploited it—the case serves as a warning that NOBUS capabilities are seriously endangered. Former senior NSA operator Jake Williams bluntly spelled out his pessimistic interpretation of the Juniper matter: "I think we can officially put the NOBUS argument to bed . . . forever."[54] Elsewhere, he spelled out why: "It's high time that US intelligence agencies admit that they are no longer the only game in town."[55]

The mysterious saga of the Shadow Brokers provides another worrying example of capable adversaries. The Shadow Brokers are an online group, assumed by some to be Russian in origin,[56] which began posting messages in August 2016. Over a series of months, they revealed a number of NSA documents and tools. Their erratic spelling and language, discussion of a fake auction of tools, and claims of non-allegiance to any nation seem like a sideshow from their two main accomplishments: attracting media attention and burning NSA capabilities by publishing them.

The most significant exploit revealed by the Shadow Brokers was an NSA exploit named ETERNALBLUE. The exploit took advantage of a part of the Windows operating

system known as Server Message Block. In effect, the exploit permitted a hacker with a foothold in the target network to compromise other computers very quickly throughout the network. The tool was so powerful that one NSA employee said, "It was like fishing with dynamite." Another employee said the intelligence gathered using the tool was "unreal."[57]

Reportedly, the NSA used the exploit in secret for five years rather than reporting it to Microsoft. This was not without risk as, had the exploit been independently discovered or stolen, many critical American computers that ran Windows would be in the line of fire. "The entire Department of Defense would be vulnerable," one NSA employee said, if the exploit got into the wrong hands.[58] But the intrusion power was too remarkable to ignore. In effect, the NSA bet that it could keep the exploit secret and that no adversary would independently discover it (at least for some period of time). This was a judgment call. Without knowing the value of the intelligence collection, it is hard to evaluate the decision.

After the Shadow Brokers gained access to NSA data, though, the danger became visible. The tool was no longer NOBUS. The NSA was aware that the value of the exploit had been "degraded" by the Shadow Brokers' access. Microsoft was then tipped off to the vulnerability by an anonymous party, likely the NSA, and issued a patch.[59] Nonetheless, a month later, hackers reengineered the ETERNALBLUE exploit for their own ends, infecting hundreds of thousands of computers that had not yet applied the patch with it. Most significantly, this forced shutdowns throughout Britain's National Health Service.[60] It is a reminder of the power of NOBUS capabilities—and the dangers that arise when they lose that special status.[61]

A similar, and perhaps related, case is the posting of CIA hacking tools by WikiLeaks in 2017. These tools, part of what the agency called Vault 7, contain exploits for a wide range of software and hardware, including devices such as smart televisions. WikiLeaks also published code from the agency that attempts to obscure the CIA's hand in operations, as well as code that attempts to evade anti-virus detection and code that handles the command and control of malicious software.[62] It is likely that all of these capabilities are substantially less valuable now that they have been revealed in public. Other actors may also try to repurpose or copy the tools for their own ends, though some of the tools seem less useful to regular hackers than to the CIA.[63] In short, the tools' NOBUS value is gone.

Increased Use of End-to-End Encryption

Cybersecurity continues to get better, albeit slowly. Companies, even those that historically had a spotty track record, now are more likely to emphasize security during the software development process. In the face of significant adversaries and increased worries about the dangers of computer hacking, the technology sector has taken significant steps to better secure code and protect user communications. Nowhere is this more obvious than in the deployment of encryption.

While in the past many communications were transmitted using insecure means, such as text messages or unencrypted web sessions, that is now less frequently the case.[64] Widely used messaging applications such as iMessage, WhatsApp, and Signal employ what is known as end-to-end encryption. This mechanism, when combined with other technologies such as public key encryption and perfect forward secrecy, substantially increases the security of communications. Modern encryption implementations forego the need for pre-shared passwords yet nonetheless change keys regularly. While encryption was once a custom technology that was cumbersome to use, today's messaging applications build it in, ensuring that users are easily protected by it, often without even knowing.

The wider deployment of secure encryption by default directly undermines two NOBUS capabilities. First, it diminishes the capacity for signals intelligence agencies to meaningfully eavesdrop on communications as they transit fiber-optic cables and other Internet chokepoints. Even when the data are encrypted without end-to-end mechanisms, the telecommunications provider is unlikely to have the decryption key. As a result, it will be unable to assist a signals intelligence agency.

Second, the deployment of end-to-end encryption renders providers like Apple and Facebook unable to turn over as much meaningful data in response to legal demands. If the data are encrypted in a way in which the providers do not have the keys, only the user and, if applicable, the intended recipient can decrypt the message. This means that government requests for information, such as under the PRISM program, are likely to be less valuable. For example, when the US government served the company that makes the secure messaging application Signal with a secret legal request, the firm was able to turn over only a small amount of information.[65] Likewise, companies are unable to help with government requests for technical assistance, such as with decrypting the phones of suspects—a fact best exemplified by the 2016 showdown

between Apple and the FBI over the work phone of one of the San Bernardino shooters.[66]

This is not to say encryption undermines all forms of intelligence collection and analysis. Usually, the encryption will obscure the content of communications but not the secondary metadata. Through legal demands and eavesdropping, a signals intelligence agency can thus often see who is communicating with whom, but not what was said. There is substantial debate on how valuable this metadata-only collection is.[67] Further, in the cases where providers do retain encryption keys, they can still turn over the data when faced with a legal demand. In some cases, such as Apple's iCloud backup mechanism, many users voluntarily put their data into environments that give providers the capacity to do this.[68]

Cryptography provides deeply significant improvements in security and has a negative impact on some NOBUS capabilities. All told, the wide deployment of encryption means that a signals intelligence agency has greater incentive to either break cryptographic implementations or illicitly access the device of either the sender or the recipient. The diminishment of some NOBUS capabilities forces greater reliance on others.

Increased Scrutiny and Demands for Overt Access

A third challenge to the NOBUS approach comes from the fact that it sometimes does not scale very well, especially not into overt environments. The NOBUS capabilities described above are often fragile, particularly those that target encryption or software vulnerabilities. Two linked trends therefore render NOBUS efforts more tenuous than ever: greater public scrutiny on signals intelligence agencies and greater law enforcement demand for similar capabilities.

Publicity has consequences. NSA documents indicate that the agency internally warns that discussion of its encryption-breaking capabilities runs the risk of their exposure or diminishment. The files caution that the capabilities "are extremely difficult and costly to acquire" and "are very fragile." Worse, this is one of the areas in which a NOBUS capability can be broken not by an adversary who matches it or understands it, but just one who learns of it. "An adversary who knows what we can/cannot break is able to elude our capabilities even without knowing the technical details of how the capabilities work," according to internal NSA documents.[69]

The need for secrecy applies broadly in signals intelligence. Speaking more generally, former National Security Council coordinator Michael Daniel said, "If you know much about it, cyber is very easy to defend against. . . . That's why we keep a lot of those capabilities very closely guarded."[70] In addition to encryption-cracking mechanisms, the necessity of covertness is perhaps especially relevant to exploitable software vulnerabilities, which patches can address.

Yet signals intelligence activities are more out in the open than ever before—as evidenced by the fact that a paper like this can be written at all. The constant drumbeat of global cybersecurity news in recent years makes it clear that there are enormous opportunities to obtain information or enable attacks. The likely result is that the NSA's targets are able to take additional steps to secure themselves and techniques that once worked will no longer be as effective. This, to some degree, is inevitable, and not the result of any one particular factor or event.

Computer hacking and other signal intelligence-like activities have explicitly become law enforcement matters as well. This forces NOBUS capabilities and discussions further out into public view and risks diminishing them. The FBI has hacked thousands of individuals around the world and retains zero day exploits for its own use.[71] Significant questions have emerged about the warrants under which the bureau did this hacking, the jurisdictional basis for authorization, and the rights of those whose computers the FBI hacked. The FBI has dismissed some of its hacking cases to avoid revealing its techniques, including zero day exploits, to defendants.[72] Suffice it to say that substantial case law is yet to come in this area. Courts will have to answer important questions about the permitted scope of law enforcement hacking and whether or how constitutional rights should interact with law enforcement capabilities and the government's associated desire for secrecy.

Law enforcement's use of tools once thought to be relevant only to signals intelligence also dramatically increases the perceived need for NOBUS capabilities against common systems, even as it diminishes the tools' power. In the context of foreign intelligence, it is likely easier to draw a distinction between the systems an agency targets and the systems an agency protects. While increasing convergence in the use of software and hardware—the impetus for the NOBUS approach—has lessened this distinction, some capabilities might still rely on it. For example, the tapping of fiber-optic cables in certain parts of the world is disproportionately likely to obtain more traffic from foreign targets than American citizens. Similarly, some software is more likely used in

China than the United States, and as such would seem more palatable to exploit. But American law enforcement is likely to investigate Americans and will want to target the very same computers that the US government has at least a nominal interest in protecting. The idealized NOBUS solution to this problem seems more necessary than ever, but also more elusive.

Conclusion: Preparing for a Future without NOBUS Capabilities

Today, there is a fundamental tension between stealing secrets and protecting secrets. Though offense and defense are not entirely at odds, signals intelligence agencies must make hard choices. The NOBUS approach is an effort to get the best of both worlds, retaining the ability to access an adversary's communications while nonetheless fostering software that is as secure as possible for a wide range of users.

Every golden age must end, and the golden age of signals intelligence is no different. The covert American head start in signals intelligence was probably always destined to become less secret and less pronounced. The rise of stronger adversaries is of obvious concern.[73] The wider deployment of encryption and the broader use of signals intelligence-like tools are trends that are more complex. These developments have demonstrably positive aspects, but they appear to pose a threat to important NOBUS capabilities that have proved useful, like passive collection. It is possible that the NSA has invented new NOBUS capabilities that overcome these trends. For example, if the NSA is able to break the common forms of cryptography, then widespread encryption does not pose a threat to passive collection. Similarly, if the agency can come up with new NOBUS techniques to replace the ones that law enforcement has adopted, then greater scrutiny on those old methods might not be as concerning. Absent another Snowden-like leak, it is impossible to resolve this uncertainty, though public statements—such as NSA Director Mike Rogers's repeated statements about the dangers of encryption—indicate that some NOBUS capabilities are under threat.

There is no silver bullet to solve this problem. The threat to NOBUS is more of an unsettling observation than it is a stirring call to a plan of action. Nonetheless, three conclusions deserve mention.

First, it is worth pausing to draw out a further point on the United States' relationship to the NOBUS idea: the same technological head start and digital pervasiveness that

enables so many NOBUS capabilities also prompts the need for it. If the United States had less to lose—if American society wasn't so thoroughly dependent on computer systems—the country wouldn't feel the same tensions between exploiting systems and securing them. A nation like North Korea, with little digital dependence, feels no such tension; to some degree, a nation like Russia might have reason to be similarly cavalier. The United States and its signals intelligence partners almost certainly feel the most pressure to develop NOBUS capabilities, scarce as those might be.

The second point is related: if NOBUS capabilities will be less plentiful, the United States should be very judicious about where it uses them. It seems apparent that many, though not all, NOBUS capabilities become less special or less effective the more they are used. Ever-stronger adversaries can discover these capabilities once deployed, as was the case with the Juniper back door and perhaps also with the Shadow Brokers. Capabilities can leak when they are used by an organization and not held closely enough. The sagas of Edward Snowden, Hal Martin, and potentially unknown others are examples of this.

Security companies and incident responders can also find and publicize the use of even advanced capabilities. A series of cybersecurity incident reports in 2015 and 2016 demonstrated this vividly and probably burned a substantial number of intelligence community capabilities thought to be NOBUS, or nearly so.[74]

Lastly, as the FBI's hacking cases show, the judicial process can cause increased public scrutiny; this scrutiny only arises when capabilities are used for law enforcement, however. All of these factors should cause the United States to use NOBUS capabilities when most needed—but only then.

If the future will yield fewer NOBUS capabilities and if they will be conserved for when they are critically important, this could lead to a reduction of overall signals intelligence capability on offense, defense, or both. The third conclusion is thus relevant: the United States will need to think more seriously about its prioritization of missions. Sometimes this notion gets presented as a hackneyed idea of directly trading off between offense and defense, but that is too simplistic. Even in an era of common software and hardware, offense and defense are not zero-sum. Intrusive hacking efforts can be used for counterintelligence purposes or to aid the defensive cybersecurity mission, for example.[75] But there is no doubt that the tension between missions exists in some form.

Understanding this tension is of vital importance. No one will feel comfortable giving up means of collecting foreign intelligence, and with good reason. Yet cases like the Juniper back door vividly demonstrate the risks of potentially overreaching. The ETERNALBLUE example further shows the complexity of the matter. It highlights the power of the right tools for intelligence collection, the dangers of those tools falling into the wrong hands, and the challenges of applying patches even when vendors are notified.

It is difficult to fully appreciate the tension between the various missions of signals intelligence using only public information. Nonetheless, it is unlikely that there are dominant strategies or easy options. For example, the NSA's move to collocate offensive and defensive teams may better position the agency to understand the trade-offs associated with certain decisions. On the other hand, the diminishment of an explicitly defensive arm may reduce the agency's credibility when engaging with companies or academia.

A better understanding of tensions between missions should serve as a foundation for shrewder prioritization. Policy makers have had to set priorities before in terms of resource allocation or staffing. This will continue, but there will also have to be new kinds of weighting as well: between doing intelligence collection covertly and attacking, for example, or between enabling intelligence collection and bolstering broader defensive efforts, or between gaining access to one class of communications and running the risk that adversaries will be able to do the same. There are real questions about oversight, civil liberties, and public accountability on all these matters, and all will have substantial impacts on citizens.

The essence of signals intelligence strategy going forward will lie in understanding and managing these tensions. NOBUS capabilities will help where they can, and should be preserved for where they can help most. But difficult decisions will still have to be made. The decline of NOBUS calls for strategic thought and guidance. The challenges involved will not submit to easy solutions, including neither the unilateral surrender of all espionage capabilities nor their unencumbered use. It may be uncomfortable to admit that some advantages once enjoyed have now been lost, but facing facts is essential. The reality is simple: the golden age has passed; the era of Nobody But Us is ending. There is no point pretending we are still alone.

NOTES

1 Timothy Mucklow, "The SIGABA/ECM II Cipher Machine: 'A Beautiful Idea,' " NSA Center for Cryptologic History, 2015.

2 For a discussion of this case, see Simon Singh, chap. 4, *The Code Book* (New York: Doubleday, 1999).

3 James Risen and Laura Poitras, "N.S.A. Report Outlined Goals for More Power," *New York Times,* November 22, 2013.

4 Dave Aitel, "Why a Global Cybersecurity Geneva Convention Is Not Going to Happen," *CyberScoop,* June 20, 2017.

5 One key American program in this effort is called BULLRUN; the corresponding British program is named EDGEHILL. Both names derive from civil war battles in the respective countries. Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times,* September 5, 2013; Jeff Larson, Nicole Perlroth, and Scott Shane, "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security," *ProPublica,* September 5, 2013.

6 Perlroth, Larson, and Shane, "N.S.A. Able to Foil Basic Safeguards"; Larson, Perlroth, and Shane, "Revealed: The NSA's Secret Campaign"; Matthew Green, "The Many Flaws of Dual_EC_DRBG," *Cryptography Engineering* (blog), September 18, 2013; Stephen Checkoway et al., "A Systematic Analysis of the Juniper Dual EC Incident," presented at Real World Crypto Symposium, 2016; Dan Shumow and Niels Ferguson, "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng," pesented at Crypto conference, August 2007; Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen, "Dual EC: A Standardized Back Door," in *The New Codebreakers,* ed. Peter Y. A. Ryan, David Naccache, and Jean-Jaques Quisquater (New York: Springer, 2016).

7 Perlroth, Larson, and Shane, "N.S.A. Able to Foil Basic Safeguards"; Larson, Perlroth, and Shane, "Revealed: The NSA's Secret Campaign."

8 Joseph Menn, "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," *Reuters,* December 20, 2013.

9 Alex Halderman and Nadia Heninger, "How Is NSA Breaking So Much Crypto?" *Freedom to Tinker,* October 14, 2015.

10 SIGINT Enabling Project, *ProPublica,* 2013; Larson, Perlroth, and Shane, "Revealed: The NSA's Secret Campaign."

11 Kevin Poulsen, "New Snowden Leak Reports 'Groundbreaking' NSA Crypto-Cracking," *Wired,* August 29, 2013; Barton Gellman and Greg Miller, " 'Black Budget' Summary Details U.S. Spy Network's Successes, Failures And Objectives," *Washington Post,* August 29, 2013.

12 National Security Agency/Central Security Service, "Exceptionally Controlled Information."

13 Halderman and Heninger, "How Is NSA Breaking So Much Crypto?"

14 For more on the interplay between encryption and software vulnerabilities in the context of state sovereignty, see Ben Buchanan, "Cryptography and Sovereignty," *Survival* 58, no. 5 (2016).

15 For more on zero days, see Leyla Bilge and Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," paper presented at 2012 Conference on Computer and Communication Security; Lillian Ablon and Timothy Bogart, "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," Rand Corporation, 2017. Bruce Schneier, "Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?" *The Atlantic,* May 19, 2014.

16 Brian Fung, "The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities," *Washington Post,* August 31, 2013.

17 Jacob Appelbaum et al., "Inside TAO: Documents Reveal Top NSA Hacking Unit," *Der Spiegel,* December 29, 2013.

18 For more, see Kim Zetter, *Countdown to Zero Day* (New York: Crown, 2014).

19 Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," *The White House* (blog), April 28, 2014.

20 Andrea Peterson, "Why Everyone Is Left Less Secure When the NSA Doesn't Help Fix Security Flaws," *Washington Post,* October 4, 2013.

21 Siobhan Gorman and Jennifer Valentino-DeVries, "New Details Show Broader NSA Surveillance Reach," *Wall Street Journal,* August 20, 2013.

22 Ewen MacAskill et al., "Mastering the internet: How GCHQ Set out to Spy on the World Wide Web," *The Guardian,* June 21, 2013.

23 Matthew Aid, "The CIA's New Black Bag Is Digital," *Foreign Policy,* July 17, 2013.

24 Laura Poitras et al., "How the NSA Targets Germany and Europe," *Der Spiegel,* July 1, 2013.

25 Ewen MacAskill et al., "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian,* June 21, 2013; James Ball, "Leaked Memos Reveal GCHQ Efforts to Keep Mass Surveillance Secret," *The Guardian,* October 25, 2013.

26 John Napier Tye, "Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans," *Washington Post,* July 18, 2014.

27 Poitras et al., "How the NSA Targets Germany and Europe."

28 MacAskill et al., "GCHQ taps fibre-optic cables"; Ball, "Leaked Memos Reveal GCHQ Efforts."

29 MacAskill et al., "GCHQ taps fibre-optic cables"; Ball, "Leaked Memos Reveal GCHQ Efforts."

30 Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *Washington Post,* October 30, 2013.

31 This was so much data that the NSA had to begin filtering some of it out right away. Barton Gellman and Matt DeLong, "How the NSA's Muscular Program Collects Too Much Data from Yahoo And Google," *Washington Post,* October 30, 2013.

32 Christian Stöcker, "GCHQ Surveillance: The Power of Britain's Data Vacuum," *Der Spiegel,* July 7, 2013. According to Bill Woodcock, president of PCH, a nonprofit Internet organization that specializes in documenting global fiber-optic infrastructure, "as much as 11 percent of global internet bandwidth travels through U.K. internet exchanges." Quoted in Richard Esposito et al., "Exclusive: Snowden Docs Reveal UK Spies Snooped on YouTube, Facebook," NBC News, January 27, 2014.

33 Ryan Singel, "NSA's Lucky Break: How the U.S. Became Switchboard to the World," *Wired,* October 10, 2007.

34 James Ball, "NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show," *The Guardian,* September 30, 2013. Barton Gellman, Ashkan Soltani, and Andrea Peterson, "How We Know the NSA Had Access to Internal Google and Yahoo Cloud Data," *Washington Post,* November 4, 2013.

35 "AT&T Whistle-Blower's Evidence," *Wired,* May 17, 2006.

36 Craig Timberg and Barton Gellman, "NSA paying U.S. Companies for Access to Communications Networks," *Washington Post,* August 29, 2013.

37 James Ball, Luke Harding, and Juliette Garside, "BT and Vodafone among Telecoms Companies Passing Details to GCHQ," *The Guardian,* August 2, 2013; Ryan Gallagher, "Vodafone-Linked Company Aided British Mass Surveillance," *The Intercept,* November 20, 2014.

38 Ball, "Leaked Memos Reveal GCHQ Efforts"; MacAskill et al., "GCHQ Taps Fibre-Optic Cables."

39 Julia Angwin et al., "NSA Spying Relies on AT&T's 'Extreme Willingness to Help,' " *ProPublica,* August 15, 2015; Sharon Goldberg, "Surveillance without Borders: The 'Traffic Shaping' Loophole and Why It Matters," The Century Foundation, June 22, 2017.

40 Ryan Devereaux, Glenn Greenwald, and Laura Poitras, "Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas," *The Intercept,* May 19, 2014.

41 Ibid.

42 Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *The Guardian,* June 7, 2013.

43 Barton Gellman and Laura Poitras, "U.S., British intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post,* June 7, 2013.

44 "NSA Slides Explain the PRISM Data-collection Program," *Washington Post,* June 10, 2013.

45 Ibid. Emphasis in the original.

46 Gellman and Poitras, "U.S., British Intelligence Mining Data."

47 Ibid.

48 Kim Zetter, "New Discovery Around Juniper Backdoor Raises More Questions About the Company," *Wired,* January 8, 2016; H. D. Moore, "CVE-2015-7755: Juniper ScreenOS Authentication Backdoor," *Rapid7* (blog), December 20, 2015; Checkoway, "A Systematic Analysis of the Juniper Dual EC Incident."

49 Thomas Fox-Brewster, "Juniper Says It Didn't Work with Government to Add 'Unauthorized Code' to Network Gear," *Forbes,* December 18, 2015.

50 Classification Guide: Project BULLRUN, National Security Agency; National Initiative Protection Program—Sentry Eagle, National Security Agency: 9.

51 Matthew Green, "On the Juniper Backdoor," *Cryptography Engineering* (blog), December 22, 2015.

52 Chris Kemmerer, "The Juniper Backdoor: A Summary," *SSL.com,* January 16, 2016.

53 Ben Buchanan, "The Legend of Sophistication in Cyber Operations," Belfer Center for Science and International Affairs, January 2017.

54 Jake Williams, "New Juniper Hack Should End NOBUS Argument Forever," *MalwareJake* (blog), December 20, 2015.

55 Jake Willliams, "Congressman Gets Mad about SS7 Flaws," *MalwareJake* (blog), April 19, 2016.

56 For one series of possible hypotheses, see Bruce Schneier, "Who Are the Shadow Brokers?'" *The Atlantic,* May 23, 2017.

57 Ellen Nakashima and Craig Timberg, "NSA officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did," *Washington Post,* May 16, 2017.

58 Ibid.

59 Ibid.

60 Nicole Perlroth and David Sanger, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool," *New York Times,* May 12, 2017.

61 Another reminder is the NSA tool known as EXTRABACON, which exploited a vulnerability in Cisco firewalls around the world. The Shadow Brokers also disclosed this capability. Chris Brook, "Cisco Warns of iOS Flaw Vulnerable to Shadowbrokers Attack," *ThreatPost,* September 19, 2016.

62 "Vault 7: CIA Hacking Tools Revealed," *Wikileaks,* news release, March 7, 2017.

63 Many of the CIA tools required physical access to the targeted device. For more on the diffusion of tools between different actors, see Ben Buchanan, "The Life Cycles of Cyber Threats," *Survival* 58, no. 1 (2016).

64 Ellen Nakashima and Barton Gellman, "As Encryption Spreads, U.S. Grapples with Clash between Privacy, Security," *Washington Post,* April 10, 2015; Nicole Perlroth, "Tech Giants Urge Obama to Reject Policies That Weaken Encryption," *New York Times,* May 19, 2015; Melanie Newman, "Encryption Risks Leading to 'Ethically Worse' Behaviour by Spies, Says Former GCHQ Chief," Bureau of Investigative Journalism, January 23, 2015.

65 Cyrus Farivar, "FBI Demands Signal User Data, but There's Not Much to Hand Over," *ArsTechnica,* October 4, 2016.

66 Dustin Volz, Mark Hosenball, and Joseph Menn, "Push for Encryption Law Falters Despite Apple Case Spotlight," *Reuters,* May 26, 2016; Joseph Menn, "Apple Says FBI Gave It First Vulnerability Tip on April 14," *Reuters,* April 26, 2016.

67 For one prominent example, see Urs Gasser et al., "Don't Panic," Berkman Center for Internet and Society, February 1, 2016.

68 This applies to regular data stored in iCloud, not passwords and other sensitive information. For more, see Michael Specter, "Apple's Cloud Key Vault, Exceptional Access, and False Equivalences," *Lawfare* (blog), September 7, 2016.

69 BULLRUN, Government Communications Headquarters: 4.

70 Danny Vinik, "America's Secret Arsenal," *Politico,* December 9, 2015.

71 Ellen Nakashima, "Meet the Woman in Charge of the FBI's Most Controversial High-Tech Tools," *Washington Post,* December 8, 2015; Mike Carter, "FBI Created Fake Seattle Times Web Page to Nab Bomb-Threat Suspect," *Seattle Times,* October 27, 2014; Nicholas Weaver, "Examining an FBI Hacking Warrant," *Lawfare* (blog), March 16, 2016; Nicholas Weaver, "The FBI's Firefox Exploit," *Lawfare* (blog), April 7, 2016.

72 Lily Hay Newman, "The Feds Would Rather Drop a Child Porn Case Than Give up a Tor Exploit," *Wired,* March 7, 2017.

73 To the extent that convergence and the other trends outlined in this paper continue, NOBUS capabilities will be both important and elusive. However, if nations take steps to try to fight convergence, such as developing their own custom software for government communications or building their own fiber-optic cable links, the situation may revert to something more similar to the SIGABA and Enigma days.

74 "Equation Group: Questions and Answers," Kaspersky Lab, February 2015; "ProjectSauron: Top Level Cyber-Espionage Platform Covertly Extracts Encrypted Government Comms," Kaspersky Lab, August 8, 2016; "The Duqu 2.0: Technical Details," Kaspersky Lab, June 11, 2015.

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

WORKS CITED

Ablon, Lillian, and Andy Bogart. "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits." Rand Corporation, 2017.

Aid, Matthew, "The CIA's New Black Bag Is Digital," *Foreign Policy,* July 17, 2013, www.foreignpolicy.com /articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation.

Aitel, Dave. "Why a Global Cybersecurity Geneva Convention Is Not Going to Happen." *CyberScoop,* June 20, 2017.

Angwin, Julia, Jeff Larson, Charlie Savage, James Risen, Henrik Moltke, and Laura Poitras. "NSA Spying Relies on AT&T's 'Extreme Willingness to Help.' " *ProPublica,* August 15, 2015, https://www.propublica.org /article/nsa-spying-relies-on-atts-extreme-willingness-to-help.

Appelbaum, Jacob, Laura Poitras, Marcel Rosenbach, Christian Stöcker, Jörg Schindler, and Holger Stark. "Inside TAO: Documents Reveal Top NSA Hacking Unit." *Der Spiegel,* December 20, 2013, www.spiegel.de /international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

Ball, James. "Leaked Memos Reveal GCHQ Efforts to Keep Mass Surveillance Secret." *The Guardian,* October 25, 2013, www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance -secret-snowden.

———. "NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show." *The Guardian,* September 30, 2013, www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year -documents.

Ball, James, Luke Harding, and Juliette Garside. "BT and Vodafone among Telecoms Companies Passing Details to GCHQ." *The Guardian,* August 2, 2013, https://www.theguardian.com/business/2013/aug/02 /telecoms-bt-vodafone-cables-gchq.

Bernstein, Daniel J., Tanja Lange, and Ruben Niederhagen. "Dual EC: A Standardized Back Door." In *The New Codebreakers,* edited by Peter Y. A. Ryan, David Naccache, and Jean-Jaques Quisguater, 256–81. New York: Springer, 2016.

Bilge, Leyla, and Tudor Dumitras. "Before We Knew It: An Empirical Study of Zero Day Attacks in the Real World." Paper presented at 2012 Conference on Computer and Communication Security.

Brook, Chris. "Cisco Warns of iOS Flaw Vulnerable to Shadowbrokers Attack." *ThreatPost,* September 19, 2016, https://threatpost.com/cisco-warns-of-ios-flaw-vulnerable-to-shadowbrokers-attack/120668/.

Buchanan, Ben. "Cryptography and Sovereignty." *Survival* 58, no. 5 (2016).

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

———. "The Legend of Sophistication in Cyber Operations." Belfer Center for Science and International Affairs, January 2017, https://www.belfercenter.org/sites/default/files/files/publication/Legend Sophistication-web.pdf.

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

Carter, Mike, "FBI Created Fake Seattle Times Web Page to Nab Bomb-Threat Suspect," *Seattle Times,* October 27, 2014, www.seattletimes.com/seattle-news/fbi-created-fake-seattle-times-web-page-to-nab -bomb-threat-suspect/.

Checkoway, Stephen, Shaanan Cohney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Maskiewicz, Eric Rescorla, Hovav Shacham, and Ralf-Philipp Weinmann. "A Systematic Analysis of the Juniper Dual EC Incident." Presented at Real World Crypto Symposium, 2016.

Daniel, Michael. “Heartbleed: Understanding When We Disclose Cyber Vulnerabilities.” *The White House* (blog), April 28, 2014, www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

Devereaux, Ryan, Glenn Greenwald, and Laura Poitras. “Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas.” *The Intercept,* May 19, 2014, https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

Esposito, Richard, Matthew Cole, Mark Schone, and Glenn Greenwald. “Snowden Docs Reveal British Spies Snooped on YouTube and Facebook.” NBC News, January 27, 2014, http://investigations.nbcnews.com/_news/2014/01/27/22469304-snowden-docs-reveal-british-spies-snooped-on-youtube-and-facebook?lite.

Farivar, Cyrus. “FBI Demands Signal User Data, but There’s Not Much to Hand Over.” *ArsTechnica,* October 4, 2016, https://arstechnica.com/tech-policy/2016/10/fbi-demands-signal-user-data-but-theres-not-much-to-hand-over/.

Fox-Brewster, Thomas. “Juniper Says It Didn’t Work with Government to Add ‘Unauthorized Code’ to Network Gear.” *Forbes,* December 18, 2015, https://www.forbes.com/sites/thomasbrewster/2015/12/18/juniper-says-it-didnt-work-with-government-to-add-unauthorized-code-to-network-gear/- 5880dadb7900.

Fung, Brian. “The NSA Hacks Other Countries by Buying Millions of Dollars’ Worth of Computer Vulnerabilities.” *Washington Post,* August 31, 2013, www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/.

Gallagher, Ryan. “Vodafone-Linked Company Aided British Mass Surveillance.” *The Intercept,* November 20, 2014, https://theintercept.com/2014/11/20/vodafone-surveillance-gchq-snowden/.

Gasser, Urs, Nancy Gertner, Jack Goldsmith, Susan Landau, Joseph Nye, David R. O’Brien, Matthew G. Olsen, Daphna Renan, Julian Sanchez, Bruce Schneier, Larry Schwartztol, and Jonathan Zittrain. “Don’t Panic.” Berkman Center for Internet and Society, February 1, 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Gellman, Barton, and Matt DeLong. “How the NSA’s Muscular Program Collects Too Much Data from Yahoo and Google.” *Washington Post,* October 30, 2013, http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/-document/p2/a129475.

Gellman, Barton, and Greg Miller, “ ‘Black Budget’ Summary Details U.S. Spy Network’s Successes, Failures and Objectives,” *Washington Post,* August 29, 2013, https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?tid=pm_world_pop.

Gellman, Barton, and Laura Poitras. “U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program.” *Washington Post,* June 7, 2013, www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Gellman, Barton, and Ashkan Soltani. “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say.” *Washington Post,* October 30, 2013, www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

Gellman, Barton, Ashkan Soltani, and Andrea Peterson. “How We Know the NSA Had Access to Internal Google and Yahoo Cloud Data.” *Washington Post,* November 4, 2013, www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.

Goldberg, Sharon. “Surveillance without Borders: The ‘Traffic Shaping’ Loophole and Why It Matters.” The Century Foundation, 2017, https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters/.

Gorman, Siobhan, and Jennifer Valentino-Devries. “New Details Show Broader NSA Surveillance Reach.” *Wall Street Journal,* August 20, 2013, http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470.

Government Communications Headquarters. BULLRUN, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0189/b2203e23.dir/doc.pdf.

Green, Matthew. “The Many Flaws of Dual_EC_DRBG.” *Cryptography Engineering* (blog). September 18, 2013, https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/.

———. “On the Juniper Backdoor.” *Cryptography Engineering* (blog), December 22, 2015, https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor/.

Greenwald, Glenn, and Ewen MacAskill. “NSA Prism Program Taps in to User Data of Apple, Google and Others.” *The Guardian,* June 6, 2013, www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Halderman, Alex, and Nadia Heninger. “How Is NSA Breaking So Much Crypto?” *Freedom to Tinker,* October 14, 2015, https://freedom-to-tinker.com/2015/10/14/how-is-nsa-breaking-so-much-crypto/.

Kaspersky Lab. “The Duqu 2.0: Technical Details.” June 11, 2015, https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

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

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

Kemmerer, Chris. “The Juniper Backdoor: A Summary,” *SSL.com,* January 16, 2016, https://www.ssl.com/article/the-juniper-backdoor-a-summary/.

Larson, Jeff, Nicole Perlroth, and Scott Shane. “Revealed: The NSA’s Secret Campaign to Crack, Undermine Internet Security,” *ProPublica,* September 5, 2013, www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications.” *The Guardian,* June 21, 2013, www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

———. “Mastering the Internet: How GCHQ Set out to Spy on the World Wide Web.” *The Guardian,* June 21, 2013, www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

Menn, Joseph. “Apple Says FBI Gave It First Vulnerability Tip on April 14.” *Reuters,* April 26, 2016, www.reuters.com/article/us-apple-encryption-fbi-disclosure-idUSKCN0XO00T.

———. “Exclusive: Secret Contract Tied NSA and Security Industry Pioneer.” *Reuters,* December 20, 2013, www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

Moore, H. D. “CVE-2015-7755: Juniper ScreenOS Authentication Backdoor.” *Rapid7* (blog), December 20, 2015, https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor.

Mucklow, Timothy, "The SIGABA/ECM II Cipher Machine: 'A Beautiful Idea,' " NSA Center for Cryptologic History, 2015, https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/assets/files/sigaba-ecm-ii/The_SIGABA_ECM_Cipher_Machine_A_Beautiful_Idea3.pdf.

Nakashima, Ellen. "Meet the Woman in Charge of the FBI's Most Controversial High-Tech Tools." *Washington Post,* December 8, 2015, https://www.washingtonpost.com/world/national-security/meet-the-woman-in-charge-of-the-fbis-most-contentious-high-tech-tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb_story.html.

Nakashima, Ellen, and Barton Gellman. "As Encryption Spreads, U.S. Grapples with Clash between Privacy, Security." *Washington Post,* April 10, 2015, https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

Nakashima, Ellen, and Craig Timberg. "NSA Officials Worried About the Day Its Potent Hacking Tool Would Get Loose. Then It Did." *Washington Post,* May 16, 2017, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

National Security Agency. Classification Guide, Project BULLRUN, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHea20.dir/doc.pdf.

National Security Agency/Central Security Service. "Exceptionally Controlled Information," https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH011c/6fb7f661.dir/doc.pdf.

National Security Agency. National Initiative Protection Program—Sentry Eagle, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHa937.dir/doc.pdf.

Newman, Lily Hay. "The Feds Would Rather Drop a Child Porn Case Than Give up a Tor Exploit." *Wired,* March 7, 2017, https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/.

Newman, Melanie. "Encryption Risks Leading to 'Ethically Worse' Behaviour by Spies, Says Former GCHQ Chief." Bureau of Investigative Journalism, January 23, 2015, https://www.thebureauinvestigates.com/2015/01/23/encryption-will-lead-to-ethically-worse-behaviour-by-spies-says-former-gchq-chief/.

Perlroth, Nicole, "Tech Giants Urge Obama to Reject Policies That Weaken Encryption." *New York Times,* May 19, 2015, www.nytimes.com/2015/05/20/technology/tech-giants-urge-obama-to-reject-policies-that-weaken-encryption-technology.html.

Perlroth, Nicole, Jeff Larson, and Scott Shane. "N.S.A. Able to Foil Basic Safeguards of Privacy on Web." *New York Times,* September 5, 2013, www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all.

Perlroth, Nicole, and David Sanger. "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool." *New York Times,* May 12, 2017, https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html.

Peterson, Andrea. "Why Everyone Is Left Less Secure When the NSA Doesn't Help Fix Security Flaws." *Washington Post,* October 4, 2013, www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws.

Poitras, Laura, Marcel Rosenbach, Fidelius Schmid, Holger Stark, and Johnathan Stock. "How the NSA Targets Germany and Europe." *Der Spiegel,* July 1, 2013, www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609-2.html.

Poulsen, Kevin. "New Snowden Leak Reports 'Groundbreaking' NSA Crypto-Cracking." *Wired,* August 29, 2013, https://www.wired.com/2013/08/black-budget/.

Risen, James, and Laura Poitras. “N.S.A. Report Outlined Goals for More Power.” *New York Times,* November 22, 2013, www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html.

Schneier, Bruce. “Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?” *The Atlantic,* May 19, 2014, www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/2/.

———. “Who Are the Shadow Brokers?” *The Atlantic,* May 23, 2017, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Shumow, Dan, and Niels Ferguson. “On the Possibility of a Back Door in the NIST SP800-90 Dual EC Prng.” Presented at Crypto conference, August 2007.

SIGINT Enabling Project, *ProPublica,* 2013, www.propublica.org/documents/item/784280-sigint-enabling-project.

Singel, Ryan. “NSA’s Lucky Break: How the U.S. Became Switchboard to the World.” *Wired,* October 10, 2007, http://archive.wired.com/politics/security/news/2007/10/domestic_taps.

Singh, Simon. *The Code Book.* New York: Doubleday, 1999.

Specter, Michael. “Apple’s Cloud Key Vault, Exceptional Access, and False Equivalences.” *Lawfare* (blog), September 7, 2016, https://www.lawfareblog.com/apples-cloud-key-vault-exceptional-access-and-false-equivalences.

Stöcker Christian. “GCHQ Surveillance: The Power of Britain’s Data Vacuum.” *Der Spiegel,* July 7, 2013, www.spiegel.de/international/world/snowden-reveals-how-gchq-in-britain-soaks-up-mass-internet-data-a-909852.html.

Timberg, Craig, and Barton Gellman. “NSA Paying U.S. Companies for Access to Communications Networks.” *Washington Post,* August 29, 2013, www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html?hpid=z3.

Tye, John Napier. “Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans.” *Washington Post,* July 18, 2014, www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

Vinik, Danny. “America’s Secret Arsenal.” *Politico,* December 9, 2015, www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331.

Volz, Dustin, Mark Hosenball, and Joseph Menn. “Push for Encryption Law Falters Despite Apple Case Spotlight.” *Reuters,* May 27, 2016, www.reuters.com/article/us-usa-encryption-legislation-idUSKCN0YI0EM.

Washington Post. “NSA Slides Explain the PRISM Data-Collection Program.” June 10, 2013, www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

Weaver, Nicholas. “Examining an FBI Hacking Warrant.” *Lawfare* (blog), March 16, 2016, https://www.lawfareblog.com/examining-fbi-hacking-warrant.

———. “The FBI’s Firefox Exploit.” *Lawfare* (blog), April 7, 2016, https://www.lawfareblog.com/fbis-firefox-exploit.

Wikileaks. “Vault 7: CIA Hacking Tools Revealed.” News release, March 7, 2017.

Willliams, Jake. “Congressman Gets Mad About SS7 Flaws.” *MalwareJake* (blog), April 19, 2016, https://malwarejake.blogspot.com/2016/04/congressman-gets-mad-about-ss7-flaws.html.

Williams, Jake. “New Juniper Hack Should End NOBUS Argument Forever.” *MalwareJake* (blog), December 20, 2015, https://malwarejake.blogspot.com/2015/12/new-juniper-hack-should-end-nobus.html.

Wired. “AT&T Whistle-Blower’s Evidence.” May 17, 2006, http://archive.wired.com/science/discoveries/news/2006/05/70908.

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

———. “Everything We Know About How the FBI Hacks People.” *Wired,* May 15, 2016, https://www.wired.com/2016/05/history-fbis-hacking/.

———. “New Discovery around Juniper Backdoor Raises More Questions About the Company.” *Wired,* January 8, 2016, https://www.wired.com/2016/01/new-discovery-around-juniper-backdoor-raises-more-questions-about-the-company/.

The preferred citation for this publication:
Ben Buchanan, **Nobody But Us: The Rise and Fall of the Golden Age of Signals Intelligence**, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1708 (August 30, 2017), available at https://lawfareblog.com/nobody-us-rise-and-fall-golden-age-signals-intelligence.

About the Author

BEN BUCHANAN

Ben Buchanan is a postdoctoral fellow at Harvard University's Cybersecurity Project, where he conducts research on the intersection of cybersecurity and statecraft. His first book, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations,* was published by Oxford University Press in 2017. He has also written on attributing cyberattacks, deterrence in cyber operations, cryptography, election cybersecurity, and machine learning. He received his PhD in war studies from King's College London, where he was a Marshall Scholar, and earned master's and undergraduate degrees from Georgetown University.

Synopsis

Traditionally, signals intelligence is neatly bifurcated into offense and defense: intercept adversaries' communication technology and protect one's own. In the modern era, however, there is great convergence in the technologies used by friendly nations and by hostile ones. Signals intelligence agencies find themselves penetrating the technologies they also at times must protect. To ease this tension, the United States and its partners have relied on an approach sometimes called Nobody But Us, or NOBUS: target communications mechanisms using unique methods accessible only to the United States. This approach, which calls for advanced methods, aims to protect communications from American adversaries, yet also ensure American access when needed. But it depends as well on a number of American advantages that are under serious threat. The decline of these advantages renews the tension between offense and defense once more. This paper examines how the NOBUS approach works, its limits, and the challenging matter of what comes next.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION