Letters, Power Lines, and Other Dangerous Things

The Politics of Infrastructure Security

The title-level DOI for this work is:

doi:10.7551/mitpress/10541.001.0001

Coda: Infrastructure as Target

The book ends right where it began: with Director of National Intelligence James Clapper's public testimony before the Senate Select Committee on Intelligence in March 2013. Clapper's testimony became infamous. Not because of the prioritization of infrastructure security that his testimony marked, but for an exchange with Senator Ron Wyden.

Senator Wyden asked Clapper: "Does the NSA [National Security Agency] collect any type of data at all on millions or hundreds of millions of Americans?"

Clapper responded: "No, sir."[1]

A few months later, this terse exchange would come under close scrutiny. In June, stories started appearing in the *Guardian* (UK) newspaper and other outlets across the globe that revealed intimate details about the United States spying apparatus.[2] NSA contractor Edward Snowden had made off with a trove of classified files that provided a glimpse into the innermost workings of the secret spying bureaucracy. The first story drawn from the Snowden leaks revealed a government order requiring Verizon to turn over phone records related to tens of millions of Americans.[3] Clapper's comments appeared in a new light. Senator Wyden later charged that Clapper's statement was baldly false and misleading. Clapper claimed that given the constraints imposed by secrecy, his answer during the public hearing had been "the least untruthful" he could provide.[4]

The *Guardian*'s phone records story was the start of a flood. The leaked documents led to story after story detailing the work of the nation's most secretive intelligence agency. The code names appeared to be straight out of a spy novel. *Bullrun*. *Mystic*. *Boundless Informant*. *Prism*. These and other previously confidential programs were discussed and picked over in public for the first time. The picture that emerged put a new spin on post-9/11 debates about infrastructure security. While most, if not all, of those earlier debates had been about protection—how to secure the vital systems

and networks that the nation relies on—under the cloak of secrecy a different set of efforts was unfolding. These newly revealed efforts were not about defense: they were about offense. The Snowden files revealed a well-financed and sprawling attempt to subvert and infiltrate digital infrastructures across the globe.

Reporting based on the leaked files revealed that the U.S. had worked to undermine encryption standards and products used worldwide. Encryption is a fundamental part of digital life. It is used to protect everything from private chats to online purchases (and a great deal more). News reports indicate that the NSA tried to undermine encryption in a number of ways, including inserting vulnerabilities into products, working with commercial vendors to encourage the adoption of weak standards that could be defeated via secret means, and interdicting and physically altering hardware.[5] The NSA reportedly spent $250 million a year to covertly influence companies to adopt designs it then could break.[6] The NSA also worked to purchase previously unknown and undisclosed software flaws—known as *zero-days*—from contractors. Zero-days are bugs that are not yet known to vendors—patches and updates are not available to mitigate these vulnerabilities. Hacking tools built on zero-days are both difficult to detect and to block.[7] According to reports linked to the Snowden documents, the NSA spent $25 million purchasing zero-days during a single year.[8]

While the U.S. government was spending billions of dollars on homeland security and prioritizing cybersecurity for critical infrastructure, it was at the same time developing policies, techniques, and technologies that undermine infrastructure security.[9] These efforts are not easily isolated.[10] The software, standards, and hardware that the NSA targets and penetrates are not only used by foreign spies, governments, and terrorists. The same technology is used inside the U.S.—by defense contractors, electric power companies, newspapers, hospitals, and ordinary users. As Bruce Schneier points out: "Because everyone uses the same software, hardware, and networking protocols, there is no way to simultaneously secure our systems while attacking their systems—whoever 'they' are."[11] Efforts targeting adversary networks can undermine U.S. interests and security. Weak encryption standards and unpatched flaws do not just mean that the U.S. can subvert foreign networks and gain valuable intelligence; it also means that U.S. companies, public-sector entities, and the everyday users that rely on these standards are also vulnerable to attack. Nothing prevents a different spy agency from finding these flaws and working to develop its own assault. It is something of a zero-sum game. As Schneier puts it: "Either everyone is more secure, or everyone is more vulnerable."[12]

The problem is complicated. The U.S. wants infrastructure security, and it also wants to collect valuable intelligence from its adversaries (and, in some cases, reserve the ability to launch attacks) at the same time. There is no simple way to untie this knot.[13] In order to ensure their own security, states will hack other states to glean important information. But this creates risks, such as inadvertent or accidental escalation. A hacking operation used to collect information might lead the target, through misunderstanding or aggravation, to respond with a more destructive move than anticipated.[14] Additionally, state-sponsored hacking campaigns risk legitimizing cyber operations, giving other countries and actors a green light to use malicious tools in new, potentially destructive ways.[15] But the use of offensive hacking tools carries another risk: the possibility or appropriation and reuse. The creation and use of these exploits and attacks might be turned back against their master.[16] The diffusion of common protocols, standards, and technology make offensive maneuvers a fraught proposition. The themes of this book now slide back into view. Decades of political and economic changes have privileged efficiency and free markets above all else. This helped drive the adoption of standard computing equipment over custom-built components in electric power. A similar story unfolded in other industries and within government. The adoption of cheap common components ties the world together in new ways—it creates a shared infrastructural public. Common software and hardware are now spread across infrastructures, making it difficult to spy on or attack adversaries without creating opportunities for them to do the same in return. A strong offense can undermine *your own* defense—while the development of a strong defensive posture can reduce *your own* ability to wage offensive campaigns.

These concerns are not idle. In 2016 a group calling themselves the Shadow Brokers appeared online.[17] They advertised what they called *cyber weapons*—tools and exploits stolen from the NSA.[18] The group, widely thought to be a front for Russian operatives, had the goods. They initially leaked exploits that targeted various network security systems.[19] Subsequent leaks made it clear that they had captured some of the NSA's most sensitive tools.[20] The Shadow Brokers were, in effect, doxing the NSA. The fallout was significant and showed the difficulties of creating offensive tools in a world that runs on shared technology. Once the tools had been publicly released, they were picked up and repurposed by various adversaries, to great effect.[21] WannaCry, a ransomware campaign built from one of these tools, spread across the globe and appeared in over 70 different countries. It was a reworking of a tool the NSA had created—named

EternalBlue—that took advantage of a flaw in Windows (the flaw is also known as EternalBlue). Microsoft had released an update to fix the flaw weeks before, but many machines remained unpatched and vulnerable.[22] WannaCry spread quickly. It hobbled the National Health Service in the UK, holding computers ransom unless its victims paid up. It affected railways, schools, and other infrastructure sectors.[23] WannaCry was not trivial. It led to between $4 billion and $8 billion in damages.[24] But things would get worse. A month after WannaCry, a new worm that also modified EternalBlue—named NotPetya—wreaked havoc. It spread first through Ukraine and then found its way into machines across the globe. As journalist Andy Greenberg's detailed rendering of the incident accounts, NotPetya affected a French construction company, a hospital in Pennsylvania, the drug company Merck, and, maybe most notably, Maersk, the world's largest container-shipping company.[25] In a flash, corporate computers and networks were rendered useless. The harm was significant. The White House estimated the total costs associated with NotPetya at $10 billion.[26] For years, observers inside and outside of government had worried that the development of offensive capabilities might boomerang and come back to haunt the U.S. Now it had.

Infrastructure security always calls for a reckoning with larger values. It asks which publics and which visions of a system *matter*. Security codifies a particular way of ordering. The ongoing development of offensive cyber capabilities may be necessary—but it is certainly fraught. It collides with the massive investment in infrastructure security that the U.S. has committed since 9/11. Sorting out this conflict—between defense and offense in a world stitched together with shared code—is an ongoing and open question. It echoes across debates about encryption policy, debates about the purchase and use of zero-day vulnerabilities, and other areas and conflicts involving state-backed hacking operations. Like the post-9/11 battles cataloged in this book, these debates will be sorted out through conflicts between competing infrastructural publics. The stakes remain high.