EDITOR HAL BERGHEL
University of Nevada, Las Vegas; hlb@computer.org

A Farewell to Air Gaps, Part 2

Hal Berghel, University of Nevada, Las Vegas

Air gaps have never been an effective deterrent to a determined state-sponsored aggressor. This is just one of the lessons we learned from Stuxnet and the Farewell incident, and I will describe a few others.

Last month we discussed two successful attempts at bridging air gaps. The first was the Reagan Administration–inspired insertion of malware into controller software supplied by Canadians to the Soviet Union for their trans-Siberian pipeline. That malware, like Stuxnet 30 years later, was specifically designed to cause the targeted systems to self-destruct. Both attacks required some means of bridging the air gaps, which in turn didn't present much of a barrier.

There were many lessons learned from these exploits. "Offense-in-depth" (the layering of offensive weapons and tactics to accomplish the objective) was the reason for Stuxnet's success. A solid foundation in experimental computing with industrial control systems was the sine qua non of this successful hack—the authors had to be solid programmers with access to a testbed of Natanz-like industrial controllers, software, and centrifuges. This fact alone considerably narrows the range of suspects. And, let's face it, burning five quasi–zero-day injectors would have been considered overkill by all but major state sponsors. From the moment Stuxnet v1.0 began unraveling in the summer of 2010, attribution was never seriously in doubt. From a political perspective, plausible deniability was instantly displaced by nonrepudiable attribution. To this day, alternative accounts haven't been offered because no one would believe them due to the overwhelming body of circumstantial evidence and indisputable political motives.

THE NEW IoT: INTERNET OF TROUBLE

The technical lessons pale in comparison to those we learned from the politics of nation-state cyberkinetic warfare strategies—which have been largely ignored by the mass media—I'll cover just a few of them.

The first lesson was that air gaps were relatively useless as a defensive layer in both the trans-Siberian pipeline and Stuxnet attacks—demonstrating that they're no match against determined state-sponsored adversaries like the Central Intelligence Agency (CIA), the National Security Agency (NSA), Israel's Mossad, and their ilk. The suggestion that an air-gap strategy alone might be sufficient to protect critical infrastructures has been a mark of the unenlightened—it was a dumb strategy in 1982, and its wisdom dropped precipitously with time.

"Offense-in-depth" was the cause of Stuxnet's success.

Air gaps are to cyberdefense what chain-link fences are to physical security—they only discourage nuisance attacks.[1] An even dumber idea is to connect critical infrastructures to the Internet. In this way, the IoT is coming to mean the *Internet of Trouble*.

Our second lesson learned was that despite the existence of state-sponsored cyberattacks[2] for well over a decade, we've taken an ostrich-like approach to the revelations. To make this point clear, let me draw your attention to the threat vectors predicted in the 1997 Marsh report:[3]

- cyberattack on specific databases,
- cyberattack for the purpose of gaining access to a network,
- cyberattack for the purpose of espionage,
- cyberattack for the purpose of shutting down service, and
- cyberattack for the purpose of introducing harmful instructions

It's as if Flame, Duqu, and Stuxnet were taken from the report's playbook, in order, 10 years later; the report also says that cyberwarfare "presents significantly new challenges for the intelligence community in identifying and assessing threats to the United States" (p. 19). Clearly, this is the case with Operation Olympic Games—the Flame and Tilded codebases used in that attack are now accessible to every digital miscreant and cyberweaponeer.

In one of life's little ironies, the US Department of Homeland Security's 2010 Cyber Storm—training exercises designed to assess the US's readiness to respond to cyberattacks—stress-tested our critical infrastructure, but failed to use the most advanced weaponry already deployed at the time (Flame, Duqu, and Stuxnet). The humor in this should not be overlooked, but, of course, Cyber Storm testing exercises—even if ineffective—do help keep the burn rate within acceptable limits, and that's what really matters to bureaucrats!

Third, the long-term implication of Stuxnet/Operation Olympic Games on the vulnerability of industrial controllers (ICs) is serious and far-reaching. ICs' general-purpose applicability means that the exploit potential of the Stuxnet family of malware extends to virtually the entire global infrastructure: transportation, energy, water supply, emergency services, and so on.

The collective vulnerability is due to the fact that ICs were manufactured with little concern for security. Although that's clearly a bad design philosophy (a brand of myopia I have labeled *technology absurdism*—that is, technology development that ignores, fails to appreciate, or underrepresents obvious negative externalities [see "Noirware," *Computer*, vol. 48, no. 3, 2015, pp. 102–107]), the ultimate in stupidity was connecting these ICs to the Internet. The problem isn't that these critical infrastructures were built around a weak security model—they were built around *no* security model. As I've said before, society should demand that companies contributing to the global infrastructure factor in potential technology abuse with the calculated velocity of innovation. ICs have been a disaster in the making for half a century. As things now stand, proper discussion of IC insecurities must include infrastructure eschatology.

Fourth, Operation Olympic Games unmistakably and recklessly pushed the world toward cyberweapons proliferation. Nuclear weapons did the same thing in the 1940s and 1950s. However, the parallel between these two eras quickly breaks down. For one thing, the concept of mutually assured destruction is meaningless without attribution—that is, retaliation in kind only makes sense if one has the "retaliatee" already in mind. Absent cyber-radar for incoming bit-bombs, no such candidate would be identifiable at the level of certainty required for any responsible retaliation.

The final lesson learned was that contemporaneous with Stuxnet/Operation Olympic Games came the burgeoning gray market in cyberweapons. Due to a robust clandestine brokerage industry, every cybermercenary, -terrorist, and -criminal in the know—not to mention government contractors and nation-states—has access to current cyberweaponry, including zero-days. This is one of the most intoxicating aspects of Operation Olympic Games. No one knows for sure how large this black market is because black budgets are classified, but it's reported that in 2013 the NSA's budget for covert purchases of software vulnerabilities from government contractors and independents was

US$25.1 million.[4] Imagine how many players are in this market in addition to the NSA.

There are three things to understand about this new digital boutique. First, it was ushered in by Stuxnet-like aggression from nation-state players. Second, this cyberweapons cottage industry was entirely predictable for anyone with even a modest knowledge of how arms races work. Third, this malware is purchased with the full understanding that it won't be reported to the software vendors who might patch their products to protect the public. Since the value of this malware to the aggressor is directly proportional to its uniqueness, novelty, effectiveness, and stealth, there's little value to nation-states and state sponsors, not to mention major cybercriminal gangs, for "used" malware.

Serious ethical questions surround the gray market in cyberweapons. Chief among them is whether a government that purports to represent its citizens should be actively involved with digital-weapons brokerages that attack their interests. There are certainly hypothetical situations where possessing invasive malware might be of use to a government—such as to avoid a terrorist attack or to interrupt an adversary's decision cycle in wartime—but that's a far cry from the tactics currently in use by the US government's three-letter agencies, which range from hacking Microsoft's BitLocker encryption system, to hacking Apple's OS updater, to spoofing Apple's Xcode iOS application development tool (https://firstlook.org/theintercept/2015/03/10/ispy-cia-campaign-steal-apples-secrets). To claim that reverse-engineering US software manufacturers' code or buying malware designed to compromise its integrity is somehow required for the sake of national security is an absurdity. The courts offer many avenues for government agencies to legally spy on citizens. The Fourth Amendment only requires the government to establish probable cause. So not only is there no major hurdle to legal surveillance, there's virtually no hurdle at all—as long as the courts approve. We need to be very clear about this: the use of digital aggression to surveil criminal suspects is ethically and legally distinct from surveilling an entire population. The former falls under the rubric of legitimate intelligence gathering, whereas the latter accompanies totalitarianism and tyranny.

President Obama's commissioned study "Liberty and Security in a Changing World" addresses gray-market malware.[5] Recommendation 30 states that

> *US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments. … We recommend that, when an urgent and significant national security priority can be addressed by the use of a Zero Day, an agency of the US Government may be authorized to use temporarily a Zero Day instead of immediately fixing the underlying vulnerability. Before approving use of the Zero Day rather than patching a vulnerability, there should be a senior-level, interagency approval process that employs a risk management approach.*

The IoT is coming to mean the *Internet of Trouble.*

The panel's five members weren't civil libertarians and constitutional scholars chosen at random; they were all handpicked by Obama. And even this coterie of loyalists couldn't abide by the current government policy on exploiting zero-day malware. It was good advice, but it was ignored.

BAD SECRETS, GOOD LEAKERS, AND MESSAGE PROSECUTIONS

Perhaps the most important consequence of these activities has nothing to do with the activities themselves but rather the biased media coverage given the partisan prosecution. Consider the case of journalist David Sanger and his anonymous source. Serious comparative analysis in context was blatantly absent.[6] It's hard to reconcile the recent selective prosecutions and jail time of Chelsea Manning, John Kariakou, Stephen Kim, Shamai Leibowits, Jeffrey Sterling, and many others[7] for leaking classified information with the near-zero accountability demanded of General David Petraeus after he pleaded guilty to the same charges.[8]

Let's examine the government's elective use of the 1917 Espionage Act morecloselybylookingatthelegalcases of Stephen Kim (http://fas.org/sgp/jud/kim/offense.pdf) and Lawrence Franklin (www.fas.org/sgp/jud/aipac/franklin_facts.pdf). Kim was convicted of giving classified information to Fox News reporter James Rosen, whereas Franklin was convicted of giving classified information to representatives of a foreign government! Kim received a 13-month prison sentence, whereas Franklin received 10 months of house arrest. The major story in my view isn't the prosecutions or lack thereof, but rather the selective, biased enforcement of laws. For a good defense these days, it's not enough to lawyer up—you also have to lobby up.

It seems very clear to me that the Espionage Act isn't used to protect national security, but rather to intimidate iconoclasts and contrarians into silence. I'll call this *message prosecution*—the point is to circumvent the Supreme Court's ban on prior restraint (censorship) by sending a clear signal to anyone who might speak out against wrongdoing to "shut up or else." I would encourage everyone to read Executive Order (EO) 13526 that covers classified national security information,[9] especially section 1.7. This EO makes it very clear that the Espionage Act and laws like it aren't supposed to be used against whistleblowers or citizens who anger the government. Nor is there any exemption for government officials who leak classified information for the political benefit of elected officials—even if authorized to do so by a sitting president! However, in these times, you're more likely to be investigated by the FBI for environmental activism than for leaking classified information on behalf of the administration.[10]

According to my college political science instructor, in the US, the principle of rule of law specifically excludes arbitrary, politically inspired, and/or self-serving enforcement, and furthermore, no person is above the law.

The current contemptuous neglect of the rule of law should make every self-respecting nomocrat puce with rage.

The current contemptuous neglect of the rule of law should make every self-respecting nomocrat puce with rage. In the words of Plato, "that state in which the law is subject and has no authority, I perceive to be on the highway to ruin."[11]

Until such time that a public interest defense is allowed under the Espionage Act by the courts (don't hold your breath on that one), I recommend that Congress amend it to include a clause faithful to the late Nebraska senator George Norris's platform on hypocrisy reduction in government, to wit: "This Act specifically exempts any person considered a political crony of the Executive Branch, or any person who leaks classified information on behalf of said Executive Branch for political advantage," thereby bringing the Act into accordance with actual practice.

MOTIVES AND MIXED MESSAGES

We pass over in silence the public's interest in the government's System Vulnerabilities Equities Policy and Process,[12] which outlines what the government does when it discovers or purchases malware that could affect the privacy and security of its citizens. All that's known at this point is that there's a policy and a process, but the details are concealed from the public (www.wired.com/wp-content/uploads/2015/03/Vulnerability-Equities-Process-Highlights-7.8.10-DOC-65-redactions_Redacted1.pdf). The default seems to be that the government feels no obligation to inform anyone about malware unless the NSA has no interest in exploiting it. This is an especially problematic stance because the government is both creating such malware and encouraging the burgeoning gray market for it. Think of the cyberweapons you could buy with the NSA's $25.1 million per annum—when the cost of each ranges from $50,000 to $100,000.[13] The public debate shouldn't be about whether this gray market should exist (that toothpaste is well out of the tube), but rather what might be done about it. At this point there's a totally hidden and unregulated, state-sponsored, worldwide malware brokerage that potentially affects the privacy and data integrity of all citizens worldwide. This is a critical issue that deserves much more investigation than it's receiving.

Related to the vulnerabilities equities policies is the fragile relationship among state-sponsored malware development, the developers and vendors of vulnerable products, and the security companies that are in the business of mitigating vulnerabilities on behalf of the customer. All three allegedly represent the same constituency, but with differing levels of integrity. Again, the extensive open public debate this should inspire is so far absent.

I conclude with a comment about the alleged motives behind Stuxnet. Without public policy discussion or congressional oversight sufficient to deflate any criticism of false dilemma, the claim that Stuxnet was the least objectionable alternative (forget optimal) exposes the claimant to ridicule.

We might never be able to debate, much less discover, the real motives behind Stuxnet. Such is life in the world of dark governments.

REFERENCES

1. R.A. Serrano and E. Halper, "Sophisticated but Low-Tech Power Grid Attack Baffles Authorities," *Los Angeles Times*, 11 Feb. 2014; www.latimes.com/nation/la-na-grid-attack-20140211-story.html.
2. R.A. Clarke and R.A. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, Ecco, 2010.
3. R.T. Marsh, "Critical Foundations Protecting America's Infrastructures," report, President's Commission on Critical Infrastructure Protection, Oct. 1997; https://fas.org/sgp/library/pccip.pdf, pp. 15–16.
4. K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, 2014.

5. R.A. Clarke et al., "Liberty and Security in a Changing World," Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 13 Dec. 2013; www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
6. F. Kaplan, "Who Leaked the Stuxnet Virus Story?," *Slate*, 28 Jun. 2013; www.slate.com/articles/news_and_politics/war_stories/2013/06/did_retired_gen_james_cartwright_leak_the_stuxnet_virus_story.2.html.
7. P. Maass, "CIA's Jeffrey Sterling Sentenced to 42 Months for Leaking to New York Times Journalist," *The Intercept*, 11 May 2015; https://firstlook.org/theintercept/2015/05/11/sterling-sentenced-for-cia-leak-to-nyt.
8. P. Thomas, M. Levine, J. Cloherty, and J. Date, "Former CIA Head David Petraeus to Plead Guilty," ABC News, 11 Mar. 2015; http://abcnews.go.com/Politics/cia-head-david-petraeus-plead-guilty/story?id=29340487.
9. "Classified National Security Information," Executive Order 13526, US White House, 29 Dec. 2009; www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information.
10. P. Lewis and A. Federman, "Revealed: FBI Violated Its Own Rules While Spying on Keystone XL Opponents," *The Guardian*, 15 May 2015; www.theguardian.com/us-news/2015/may/12/revealed-fbi-spied-keystone-xl-opponents.
11. Plato, "Book IV," *Laws*, Project Gutenberg; www.gutenberg.org/files/1750/1750-h/1750-h.htm.
12. K. Zetter, "Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA," *Wired*, 15 Apr. 2014; www.wired.com/2014/04/obama-zero-day.
13. A. Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," *Forbes*, 23 Mar. 2012; www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits.

HAL BERGHEL is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.