REFLECTIONS ON DISRUPTION: CYBERWEAPONS

Nicole Perlroth

Over the last few years, my research has focused on the black market for something called a zero day vulnerability, which a lot of people were not familiar with—or at least they weren't four years ago. These days people are more familiar with this market thanks to an Apple–FBI–Department of Justice case a little over a year ago, when the DOJ sought in court to force Apple to create a backdoor into an iPhone used by one of the gunmen in the San Bernardino, California, shootings. If you remember, the DOJ officials ended up actually dropping the case. They said, "No, thanks. We don't need your help anymore. We actually were able to find a way into the phone through an outside party."

That outside party had found what's called a "zero day," which is just an unknown vulnerability in hardware or software that has not been patched and functions as a kind of invisible backdoor that allowed the government to get into this iPhone, and potentially many, many others.

Those weapons—zero days—can be used as espionage tools or as access points to drop more malicious, destructive cyberweapons, and they exist in much of the widely used software we rely on today. Some of the most coveted, for example, are in Apple and Microsoft software. One zero day hole in that software can fetch a million dollars in some cases on the black market—where governments, including our own, are actively paying hackers to turn over holes in this software and agree never to disclose them to the software maker for patching (which would render a zero day useless).

For the past few years, I've taken a deep dive into this market, its origins, and how it was catalyzed by the US government. One of the things that has been interesting is that Stuxnet, for all its publicity, did not just hit the computers that control Iranian centrifuges. It hit computers in thirty-one countries—and opened other countries' eyes to what these cyberweapons can do, the possibilities of offensive capabilities in cyberspace. It also jump-started the appetite for other countries to acquire their own stockpiles of cyberweapons and the means to deploy them.

In cyber, the countries that have the advanced capabilities to do harm are generally thought to be "the original five"—the United States, Russia, Israel, China, and the United Kingdom. Then we also have "the other five" players that have high intent to do harm, but capabilities that range from rudimentary, junior high–level skills to semi-advanced. This group generally includes North Korea and Iran, the Islamic State, al-Qaeda, and perhaps the Taliban.

But the problem is that the always-tenuous gap is closing between countries that have low intent and high capability, and the second group of actors with high intent and low capability. The reason that gap is closing is in part because of the market for zero days and other tools that can be easily acquired on the growing black market. There are now companies out there that sell "press and play" capabilities, particularly for cybersurveillance, maybe not yet for cyberweapons, who are actively marketing their services to countries that have the willpower, but not the talent or skills, to do actual harm.

As an interesting anecdote, I went down to Argentina to meet with the hacker community, in large part because the Argentine population is highly educated but their access to technology is fairly limited because of trade restrictions. To get access to certain apps and games, Argentine youth must learn how to hack. So the country has a very interesting culture of hacking. Many of them are naturally quite good at finding these vulnerabilities and zero days. And because of the currency exchange rates, if they sell one zero day to a nation-state broker for five or six figures, they can live pretty large in the trendy Palermo neighborhood of Buenos Aires.

I asked one of these hackers, “Who won’t you sell to? Will you only sell to ‘good’ Western governments?” They said, “Nicole, you cute thing, you have to realize that we’re in Argentina. We’re not necessarily your ally, and the last time we checked, the country that bombed another country into oblivion wasn’t Iran or North Korea. So we’ll just sell to whoever has the biggest bag of cash.”

When we talk about a “strategy-free zone” and national security issues, one of the things that has happened just over the last year, which has been catastrophic, was the Shadow Brokers leaks. Some of the NSA’s own zero day and cyber arsenal was stolen and dumped online by a group calling themselves the Shadow Brokers. By most accounts, the NSA still does not know who exactly the Shadow Brokers are—it believes they are a combination of an insider and a nation-state, almost certainly Russia—but once the NSA’s tools were leaked online, they could be used by anyone.

In one case, they were picked up in a widespread attack by North Korean attackers, called “WannaCry.” You may recall a few months ago there was an attack that suddenly froze computers with ransomware, and attackers demanded a ransom in bitcoin to unlock a compromised user’s data. The attack hit major companies in Russia, the United States, and Europe, and even shut down hospitals in Britain.

A week or so later, we saw a similar attack, using the same NSA tools, on a Ukrainian payroll system that appeared to be a targeted attack by Russian hackers on Ukraine. But what the attack demonstrated was that we’re now in a globalized system, where lots of international companies actually pay contractors in Ukraine as part of their day-to-day business. Suddenly you saw Merck, Maersk, even companies in Tasmania paralyzed—having been taken down by a Russian attack using leaked NSA tools.

* * *

What do we do about this?

There is not much good news to report in this arena, though what I call "the resistance movement" has started taking shape in Silicon Valley. Recently I spent a lot of time in the bowels of Google, which has started a program to pay hackers bounties for turning over vulnerabilities in Google code. Google is paying them sums of money that are not as high as what nation-states will pay hackers, but it's paying more on the front end to keep hackers from weaponizing their code. For example, typically a nation-state or nation-state broker will require hackers to demonstrate how their zero day can be "weaponized" into an espionage tool or cyberweapon. But that takes time for testing and development, often months. By paying hackers just for the vulnerability alone, Google makes sure the vulnerability gets fixed and patched before it ever gets weaponized, and saves hackers some time.

Google has also started a project called Project Zero. It culled some of the best employees on its security team and hired hackers who have turned over bugs to its own bug bounty program, and essentially charged them with a mission to go around the internet, finding vulnerabilities in widely used products and code, in an effort to get them patched. The program is a bright light on the defense side of things.

But the United States is woefully behind in defense. For every one person working on information assurance and resilience at the NSA, there are eighteen people working on how to exploit code for information collection. That is the gap we are dealing with.

As far as international cooperation, the problem is that the United States does not have much ground to stand on. The US government has been actively exploiting software and paying hackers to turn over gaping security holes in their products for two decades now. It is not going to stop looking for zero days or exploiting them anytime soon. And, God forbid, if a terrorist attack were to happen tomorrow, and it turned out we could have somehow stopped it by getting into someone's encrypted iPhone to read the planning messages ahead of time—well, critics would call the NSA or maybe even the US government negligent for not doing more to get into that phone or computer operating system.

Importantly, as likely users of these weapons ourselves, we Americans have early on lost our halo on this topic. This market has spread far beyond US borders, where people are willing to sell these vulnerabilities to nation-states like Russia, Iran, or North Korea that have a very different moral compass and strategic calculation for how they will be used. This is a global problem, and solutions are hard to come by. It is not clear whether any kind of international code of conduct would work, but my point in doing this research is to compel governments to at least stop pretending these programs do not exist and start having the necessary conversations.

What I found in the zero day market realm is that people are not having these discussions, in part because data are logically hard to come by. The second you talk about one of these vulnerabilities, it gets patched, and suddenly a good that was worth a million dollars is now worth nothing. The United States and other countries are pouring millions into these programs, and the last thing they want is to see their espionage diamonds turned to mud.

But I think that ultimately the best way forward is to get this out in the open, admit that this is something we're doing, admit that it has crawled far beyond our borders, and try to organize settings—like this one—to talk openly about what is an acceptable use of these vulnerabilities and what is not an acceptable use. Or at least, inside the United States, we need to talk about the fact that we are clearly not protecting these methods enough from groups, like the Shadow Brokers, who are dumping them online and allowing our adversaries to use them back against us.

* * *

Unfortunately, I think that extrapolating nuclear weapons deterrent strategies to the cyberdomain won't work. One problem is determining attribution for any attack, which is a technically hard problem to either do today or create network architectures over time that could help. But deterrence is deficient also in large part because we are operating on a very asymmetrical battlefield. Yes, the United States is still the most advanced when it comes to offensive capabilities. But we are also the most vulnerable, because we are the most hyperconnected. Meanwhile, an adversary like North Korea has a very weak connection to the internet and is nowhere near as vulnerable as we are to cyberattack. So it's a very asymmetrical situation we find ourselves in.

One of the other things I would point to is that North Korea and Iran are heavily investing in their own offensive capabilities because they know they'll never be able to match us with kinetic warfare. We are all focused on mushroom clouds at the moment, particularly when we talk about North Korea and Iran, but no one's really focused on the fact that North Korea spent the better part of the last five years planting software "implants" in South Korea's critical infrastructure in the event of a rainy day, or kinetic escalation. Researchers have found evidence that Pyongyang's hackers have been exploiting vulnerabilities in South Korean systems and implanting malicious code at South Korean banks, utilities, and major companies that are the equivalent of "logic bombs" that can be launched to shut down South Korean systems, wipe data, paralyze South Korea's economy, or, in the worst case scenario, turn its power off.

We don't know yet how good they are at some of those offensive capabilities, but we know they now have NSA capabilities in their arsenal, and we know they've been actively infiltrating these systems for the past five years, so that's the situation we now find ourselves in.

Of course it wouldn't be novel to use a cyberweapon to target physical infrastructure. We've all been doing it to each other for the last decade. In fact, Russia has been actively targeting US energy networks and US energy companies and, most recently, some nuclear plants—not at the production level yet, but at the employee level—with increasing frequency. Their ultimate goals are not known, but it doesn't look like they are out to steal trade secrets. It looks more like the type of attack where they're laying the eventual groundwork for a future attack. China has been caught breaking into the computerized systems we use to control our industrial control systems as well.

I have zero doubts that the United States is doing the same. So perhaps we have reached a détente. We're all so implanted in each other's systems that we know the minute we launch something, they'll launch it back, or vice versa, which brings us full circle to mutually assured destruction.