WHAT IS TO BE HACKED?

At the beginning of 2017 information security researcher, Amnesty International technologist, and hacker Claudio ("nex") Guarnieri launched "Security without Borders," an organization devoted to helping civil society deal with technical details of information security: surveillance, malware, phishing attacks, etc. Journalists, activists, nongovernmental organizations (NGOs), and others are all at risk from the same security flaws and inadequacies that large corporations and states are, but few can afford to secure their systems without help. Here Guarnieri explains how we got to this stage and what we should be doing about it.

COMPUTER SYSTEMS WERE DESTINED FOR a global cultural and economic revolution that the hacker community long anticipated. We saw the potential; we saw it coming. And while we enjoyed a brief period of reckless banditry, playing cowboys of the early interconnected age, we also soon realized that information technology would change everything, and that information security would be critical. The traditionally subversive and anti-authoritarian moral principles of hacker subculture increasingly have been diluted by vested interests. The traditional distrust of the state is only meaningfully visible in some corners of our community. For the most part—at least its most visible part—members of the security community/industry are enjoying six-figure salaries, luxurious suites in Las Vegas, business class traveling, and media attention.

The internet has morphed with us: once an unexplored space we wandered in solitude, it has become a marketplace for goods, the primary vehicle for communication, and the place to share cat pictures, memes, porn, music, and news as well as an unprecedented platform for intellectual liberation, organization, and mobilization. Pretty great, right? However, to quote Kevin Kelly:

> *There is no powerfully constructive technology that is not also powerfully destructive in another direction, just as there is no great idea that cannot be greatly perverted for great harm.... Indeed, an invention or idea is not really tremendous unless it can be tremendously abused. This should be the first law of technological expectation: the greater the promise of a new technology, the greater is the potential for harm as well* (Kelly 2010:246).

Sure enough, we soon observed the same technology of liberation become a tool for repression. It was inevitable, really.

Now, however, there is an ever more significant technological imbalance between states and their citizens. As billions of dollars are poured into systems of passive and active surveillance—mind you, not just by the United States, but by every country wealthy enough to do so—credible defenses either lag, or remain inaccessible, generally only available to corporations with deep enough pockets. The few ambitious free software projects attempting to change things are faced with rather unsustainable funding models, which rarely last long enough to grow the projects to maturity.

Nation states are well aware of this imbalance and use it to their own advantage. We have learned through the years that technology is regularly used to curb dissent, censor information, and identify and monitor people, especially those engaged in political struggles. We have seen relentless attacks against journalists and activists in Ethiopia, the crashing of protest movements in Bahrain, the hounding of dissidents in Iran, and the tragedy that became of Syria, all complemented with electronic surveillance and censorship. It is no longer hyperbole to say that people are sometimes imprisoned for a tweet.

As a result, security can no longer be a privilege, or a commodity in the hands of those few who can afford it. Those who face imprisonment and violence in the pursuit of justice and democracy cannot succeed if they do not communicate securely, or if they cannot remain safe online. Security must become a fundamental right to be exercised and protected. It is the precondition for privacy, and a key enabler for any fundamental freedom of expression. While the security industry is becoming increasingly dependent—both financially and politically—on the national security and defense sector, there is a renewed need for a structured social and political engagement from the hacker community.

Some quarters of the hacker community have long been willing to channel their skills toward political causes, but the security community lags behind. Eventually some of us become mature enough to recognize the implications and social responsibilities we have as technologists. Some of us get there sooner, some later; some never will. Having a social consciousness can even be a source of ridicule among techies. You can experience exclusion when you become outspoken on matters that the larger security and hacking communities deem foreign to their competences. Don't let that intimidate you.

As educated professionals and technicians, we need to recognize the privilege we have, like our deep understanding of the many facets of technology; we must realize that we cannot abdicate the responsibility of upholding human rights in a connected society while continuing to act as its gatekeepers. Whether creating or contributing to free software, helping someone in need, or pushing internet corporations to be more respectful of users' privacy, dedicating your time and abilities to the benefit of society is concretely a political choice and you should embrace that with consciousness and pride.

TODAY WE FACE UNPRECEDENTED challenges, and so we need to rethink strategies and re-evaluate tactics.

In traditional activism, the concept of "bearing witness" is central. It is the practice of observing and documenting a wrongdoing, without interfering, and with the assumption that exposing it to the world, causing public outcry, might be sufficient to prevent it in the future. It is a powerful and, at times, the only available and meaningful tactic. This wasn't always the case. In activist movements, the shift of tactics is generally observed in reaction to the growth, legitimization, and structuring of the movements themselves as

they conform to the norms of society and of acceptable behavior.

Similarly, as we conform too, we also "bear witness." We observe, document, and report on the abuses of technology, which is a powerful play in the economic tension that exists between offense and defense. Whether it is a journalist's electronic communications intercepted or computer compromised, or the censorship of websites and blocking of messaging systems, the exposure of the technology empowering such repressions increases the costs of their development and adoption. By bearing witness, such technologies can be defeated or circumvented, and consequently re-engineered. Exposure can effectively curb their indiscriminate adoption, and factually become an act of oversight. Sometimes we can enforce in practice what the law cannot in words.

The case of Hacking Team is a perfect example. The operations of a company that produced and sold spyware to governments around the world were more effectively scrutinized and understood as a result of the work of a handful of geeks tracking and repeatedly exposing to public view the abuses perpetrated through the use of that same spyware. Unfortunately, regulations and controls never achieved quite as much. At a key moment, an anonymous and politicized hacker mostly known by the moniker "Phineas Phisher" (Franceschi-Bicchierai 2016) arrived, hacked the company, leaked all the emails and documents onto the internet, and quite frankly outplayed us all. Phineas, whose identity remains unknown almost two years later, had previously also hacked Gamma Group, a British and German company and competitor of Hacking Team, and became a sort of mischievous hero in the hacktivist circles for his or her brutal hacks and the total exposure of these companies' deepest secrets. In a way, one could argue that Phineas achieved much more attention from the public, and better results, than anyone had previously, myself included. Sometimes an individual, using direct action techniques, can do more than a law, a company, or an organization can.

However, there is one fundamental flaw in the practice of bearing witness. It is a strategy that requires accountability to be effective. It requires naming and shaming. And when the villain is not an identifiable company or an individual, none of these properties are available to us in the digital world. The internet provides attackers plausible deniability and an escape from accountability. It makes it close to impossible to identify them, let alone name and shame them. And in a society bombarded with information and increasingly reminded by the media of the risks and breaches that happen almost daily, the few stories we do tell are becoming repetitive and boring. After all, in front of the "majesty" of the Mirai DDoS attacks (Fox-Brewster 2016), or the hundreds of millions of online accounts compromised every other week, or even in front of the massive spying infrastructure of the Five Eyes (Wikipedia 2017c), who in the public would care about an activist from the Middle East, unknown to most, being compromised by a crappy trojan (Wikipedia 2017d) bought from some dodgy website for 25 bucks?

We need to stop, take a deep breath, and look at the world around us. Are we missing the big picture? First, hackers and the media alike need to stop thinking that the most interesting or flamboyant research is the most important. When the human rights abuses of HackingTeam or FinFisher are exposed, it makes for a hell of a media story. At times, some of the research I have coauthored has landed on the front pages of major newspapers. However, those cases are exceptions, and not particularly representative of the reality of technology use as a tool for repression by a state. For every dissident targeted by sophisticated commercial spyware made by a European company, there are hundreds more infected with free-to-download or poorly written trojans that would make any security researcher yawn. Fighting the illegitimate hacking of journalists and dissidents is a never-ending cat and mouse game, and a rather technically boring one. However, once you get past the boredom of yet another DarkComet (Wikipedia 2017b) or Blackshades (Wikipedia 2017a) remote administration tool (RAT), or a four-year-old Microsoft Office exploit, you start to recognize the true value of this work: it is less technical and more human.

I have spent the last few years offering my expertise to the human rights community. And while it is deeply gratifying, it is also a mastodontic struggle. Securing global civil society is a road filled with obstacles and complications. And while it can provide unprecedented challenges to the problem-solving minds of hackers, it also comes with the toll of knowing that lives are at stake, not just some intellectual property, or some profits, or a couple of blinking boxes on a shelf.

How do you secure a distributed, dissimilar, and diverse network of people who face different risks, different adversaries, and operate in different places, with different technologies, and different services? It's a topological nightmare. We—the security community—secure corporations and organizations with appropriate modeling, by making uniform and tightening the technology used, and by watching closely for anomalies in that model. But what we—the handful of technologists working in the human rights field—often

do is merely "recommend" one stock piece of software or another and hope it is not going to fail the person we are "helping."

For example, I recently traveled to a West African country to meet some local journalists and activists. From my perennial checklist of technological solutionism to preach everywhere I go, I suggested to one of these activists that he encrypt his phone. Later that night, as we met for dinner, he waved his phone at me upon coming in. The display showed his Android software had failed the encryption process, and corrupted the data on his phone, despite his having followed all the appropriate steps. He looked at me and said: "I'm never going to encrypt anything ever again." Sometimes the technology we advocate is inadequate. Sometimes it is inaccessible, or just too expensive. Sometimes it simply fails.

However, tools aside, civil society suffers a fundamental lack of awareness and understanding of the threats it faces. The missing expertise and the financial inability to access technological solutions and services that are available to the corporate world certainly isn't making things any easier. We need to approach this problem differently, and to recognize that civil society isn't going to secure itself.

To help, hackers and security professionals first need to become an integral part of the social struggles and movements that are very much needed in this world right now. Find a cause, help others: a local environmental organization campaigning against fracking, or a citizen journalist group exposing corruption, or a global human rights organization fighting injustice. The help of security-minded hackers could make a significant impact, first as a conscious human being, and only second as a techie, especially anywhere our expertise is so lacking.

And second, we need to band together. Security Without Borders is one effort to create a platform for like-minded people to aggregate. While it might fail in practice, it has succeeded so far in demonstrating that there are many hackers who do care. Whatever the model will be, I firmly believe that through coordinated efforts of solidarity and volunteering, we can make those changes in society that are very much needed, not for fame and fortune this time, but for that "greater good" that we all, deep down, aspire to. ■

CLAUDIO GUARNIERI, *aka Nex, is a security researcher and human rights activist. He is a technologist at Amnesty International, a researcher with the Citizen Lab, and the co-founder of Security Without Borders.*

BIBLIOGRAPHY

Fox-Brewster, Thomas. 2016. "How Hacked Cameras are Helping Launch the Biggest Attacks the Internet Has Ever Seen." *Forbes*, September 25. https://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#32d0f3c35899

Franceschi-Bicchierai, Lorenzo. 2016. "Hacker 'Phineas Fisher' Speaks on Camera for the First Time—Through a Puppet." *Motherboard*, July 20. https://motherboard.vice.com/en_us/article/hacker-phineas-fisher-hacking-team-puppet

Kelly, Kevin. 2010. *What Technology Wants*. New York: Viking Press.

Wikipedia. 2017a. "Blackshades." Wikipedia, last updated March 23. https://en.wikipedia.org/wiki/Blackshades

———. 2017b. "DarkComet." Wikipedia, last updated May 14. https://en.wikipedia.org/wiki/DarkComet

———. 2017c. "Five Eyes." Wikipedia, last updated April 19. https://en.wikipedia.org/wiki/Five_Eyes

———. 2017d. "Trojan horse." Wikipedia, last updated May 12. https://en.wikipedia.org/wiki/Trojan_horse_(computing)