Hacking Back unpacked: an eye for an eye? Not so fast

Stefan Soesanto | Senior Researcher, Cyber Defense Team, ETH Zurich | @iiyonite

Theme

It had to happen eventually. Out of all the countries in the world, the hacking back debate has finally entered the political discourse in neutral Switzerland. While it is still too early to determine where the discussion will be heading toward, it is also the perfect time to insert a new perspective on hacking back.

Summary

This analysis will try to build a new baseline by explaining the fragmented history of hacking back and outlining varying degrees of operational intensity to refine a more nuanced understanding of hacking back.[1] Having said that, given the small number of publicly known cases, writing about hacking back is similar to putting together a 1000-piece puzzle with a mere 20 pieces while having only a rough idea as to what the complete picture actually looks like.

Analysis

The Swiss discourse on hacking back was kicked off by Sanija Ameti, a PhD researcher at the institute for public law at the University of Bern, with an op-ed in the Neue Zurcher Zeitung (NZZ) on July 17, 2020.[2] Ameti's core argument is that a solely defensive stance, that requires companies to invest large chunks of their profits to continuously up their cybersecurity posture, is both unrealistic in the long run and insufficient in the short term, particularly when it comes to defending again nation state actors. Her solution: private companies ought to be allowed to build-up their own active cyber defence capabilities, or outsource hacking back operations to specialized companies, whose activities could be overseen by the Swiss defence department.

Two weeks later, the NZZ published a counter-op-ed by IT entrepreneur Fabian Reinhard.[3] Reinhard argued that companies have already adapted to the evolving cyber threat landscape by implementing defence in-depth strategies. Additionally, he notes that allowing companies to build-up and acquire offensive capabilities would be synonymous to militarizing cyberspace and kicking-off an arms race. Reinhard's solution: Focus on

[1] For an analysis on the ethical and legal questions surrounding hacking back see: Patrick Lin, 'Ethics of Hacking Back,' California Polytechnic State University, September 26, 2016. Scott J. Shackelford et al., 'Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking,' University of Pennsylvania Journal of International Law, 2019.

[2] Sanija Ameti, 'Cyberangriff – die bessere Verteidigung?' NZZ, July 17, 2020.

[3] Fabian Reinhard, ‚Der digitale Gegenangriff ist keine brauchbare Strategie für die Cyber-Verteidigung,' NZZ, August 1, 2020.

international cooperation to hunt down cybercriminals and maybe even create an international cybersecurity alliance to enhance the private sector's defensive posture.

On November 5, 2020, broadcasting company SRF reinvigorated the discussion by interviewing two members of the Swiss Federal Assembly.[4] Jörg Mäder – who is also a freelance programmer – did not like Sanija's idea and explained that cyberspace should not degenerate into vigilante justice. As a solution he emphasized that the government and private sector should act as a team and play to their strengths within a clearly regulated framework. Meanwhile, Assembly member Franz Grüter – who is also the chairman of an IT company – voiced some understanding for Sanija's position by noting that the very idea of hacking back arises due to a certain discomfort within the private sector pertaining to the current status quo. As a solution, he noted that the federal government should further expand its competencies.

Overall, the Swiss hacking back debate largely follows in the same footsteps and argumentative patterns of similar discussions abroad - particularly in the United States - over the past two decades. Subsequently, so far there has not been an argument that might possibly push the hacking back discussion to the next level. So, let us try to fix that.

From the onset we have to be clear about the terminology we are using. Hacking back has nothing to do with Active Cyber Defense (ACD). In fact, ACD is so ill-defined that it means different things to different people at different times in different places. For the US Department of Defense, ACD synchronizes real-time detection, analysis, and mitigation of threats to critical networks and systems. And even though ACD "is active within the networks it protects, it is not offensive and its capabilities affect only the networks where they have been installed by network operators and owners."[5] On the other end of the equation are people like Gary McGraw, then Chief Technology Officer at Cigital, who wrote in TechTarget seven years ago that, "any active defence strategy is going to involve the use of a security hole that is exploited on the original attacker's system."[6] Even Washington Post's Ellen Nakashima had a hard time figuring out back in 2013 what ACD actually encompassed, noting that "in the parlance of network security, digital deception is known as a type of 'active defense,' a controversial and sometimes ill-defined approach that could include techniques as aggressive as knocking a server offline."[7] One look at the Wikipedia pages on 'active defense,' 'proactive cyber defense,' and 'cyber self-defense' ought to be enough to confuse any reader on the coherence of the ACD term and its popular usage.[8] The bottom line is this: hacking back has nothing to do with defence no matter how many adjectives we slap in front of it. Hacking back is

[4] Curdin Vincenz, 'Angriff als beste Verteidigung gegen Hacker,' *SRF*, November 5, 2011.

[5] NSA, 'Active Cyber Defense (ACD),' NSA/CSS, August 4, 2015. https://apps.nsa.gov/iaarchive/programs/iad-initiatives/active-cyber-defense.cfm

[6] Gary McGraw, 'Cyberwar calls for software and system investment, not hacking back,' *TechTarget*, March 2013.

[7] Ellen Nakashima, 'To thwart hackers, firms salting their servers with fake data,' *The Washington Post*, January 2, 2013.

[8] Wikipedia, 'Proactive Cyber Defence.'; Wikipedia, 'Active Defense.'; Wikipedia, 'Cyber Self-Defense.' Note: It is rather ironic that there is literally no Wikipedia page on the specific term 'active cyber defense'

offensive. Hacking back is aggressive. And hacking back plays by different rules than classical network defenders do. Period.

Three cases-studio of hacking back

We also have to be clear about what exactly we mean by hacking back. But before we embark on that journey, let us first add some context by looking at three historical cases that – in my opinion – have significantly shaped our understanding of what hacking back encompasses today.

The first case is found in Cliff Stoll's 1989 book The Cuckoo's egg.[9] For those who have not yet read it: read it. It is a classic and an amazing read. Suffice to say, at one point in Cliff's adventure, he decides to figure out whether it would be possible for an adversary to gain access to the network of the MITRE Corporation, and thereby use MITRE as a hub to dial out into other networks – including Berkeley where Cliff himself was sitting and seeing the adversary connecting to his system from MITRE. As he describes it in his own words: "I'd go home and try to use the international data communication network Tymnet to connect to MITRE, trying to break into a place I wasn't supposed to be." So, on the next day, Cliff dials into MITRE's internal network. No password required. He then dials out into Berkeley and is able to connect – confirming his 'hub' hypothesis. At this point, Cliff could have just exited MITRE's network, but he did not. He went on to access MITRE's Aerovax system through a guest account. Again, no password necessary. Then by pure coincidence he stumbles upon a trojan horse the adversary deployed to collect login information from MITRE's legitimate users. Overall, as Cliff puts it, "I remember an hour poking around MITRE's internal network. At once it felt exciting and forbidden. Any minute, I expected someone to send a message on my computer screen, 'We caught you. Come out with your hands up.'" The following day, Cliff decided to call up his contact at MITRE, hinting at the trojan horse in their system. But as Cliff himself explained, "I couldn't admit that I'd danced through his system yesterday, discovering the Trojan Horse."[10]

What Cliff did, would be considered a classical hack back in the old days. Yet from today's perspective, would anyone judge Cliff's actions as illegal and subsequently sentence him to pay a fine or even go to prison? Maybe… but highly likely not.

The second case occurred in June 1998, when the security researcher and former FBI informant Max Ray Butler exploited a vulnerability – which was discovered three months earlier - in a piece of software called the BIND 'named' domain server. According to Kevin Poulson over at Securityfocus, Butler was concerned that government networks would not patch the vulnerability and thus decided to launch "a program that scanned for vulnerable Defense Department systems, cracked them, then closed the hole in each of them -- forestalling attacks from other hackers. Less altruistically, Butler's program created a back door on every system it penetrated, which the hacker could have used to gain access later." In 2001, Butler was sentenced to 18 months in prison. Being

[9] The book is based on the well-known investigation of the author at the Lawrence Berkeley National Laboratory to discover the hacker Markus Hess in 1986.

[10] Clifford P. Stoll, 'The Cuckoo's Egg,' Pocket Books 1989, pp. 150-153.

interviewed in jail, Butler noted that, "I knew that I shouldn't have been doing what I was doing, but I had good intentions overall, and I closed this hole in thousands of systems, probably tens of thousands of systems."[11]

By today's standards we would not consider this case to fall in the hack back category. Instead, most security researchers would categorize Butler's actions as a white hat gone grey. So why did I include the case in the list? You will see later.

The last historical case is probably also the most famous one. Back in 2003, Shawn Carpenter worked as a security analyst for Sandia National Laboratories, which at the time was a wholly owned subsidiary of defence contractor Lockheed Martin. When numerous systems crashed at Lockheed's Orlando office, he and his team helped investigate the incident and discovered the presence of multiple rootkits and files ready for exfiltration. Eager to figure out who exactly was responsible for this campaign, Carpenter pitched the idea of a hacking back operation to management. Naturally, management refused as they were neither eager to violate the Computer Fraud and Abuse Act (CFAA), draw attention to the breach, nor had any appetite to invite additional attacks by the same threat actor. With his idea official shot down, Carpenter nonetheless embarked on his own secret hacking back project by preparing honeypots stacked with declassified government documents on his made-up contractor replica system. Luckily, the threat actor took the bait and led Carpenter to identify a hop-off server in South Korea - whose password he brute forced – filled with tools and gigabytes of stolen documents from various US defence programs. After 10 months of investigation, Carpenter's trail inevitably ended at three routers in the province of Guangdong, China.[12] Weary of sharing his findings with Sandia or Lockheed, he approached the FBI and US Army Counterintelligence who used his information to feed into "eight open cases throughout the United States," including "at least three clandestine Army operations."[13] In fact, Carpenter succeeded in tracking one the earliest Chinese espionage campaigns into US defence industrial base networks, now famously dubbed operation Titan Rain.[14]

When the FBI informed Sandia of Carpenter's hacking back project, he was immediately fired for "'being insubordinate,' in 'violation of the law,' and for the 'utilization of Sandia information outside of Sandia.'"[15] Carpenter took his wrongful termination case to court and in 2007 a jury awarded him $4.3 million in damages.[16] Reflecting in 2018 on his hacking back operation, Carpenter explained that "there's a lot of luck involved, because you don't know what other operations may be going on," adding that "I'm a lot more measured now."[17] Carpenter's adventure is the prototype example of a hacking back

[11] Kevin Poulson, 'Max Vision begins 18-month term,' *Securityfocus*, July 5.

[12] Nathan Thornburgh, 'The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),' *Time*, September 5, 2005.

[13] Nicholas Schmidle, 'The Digital Vigilantes Who Hack Back,' *The New Yorker*, April 30, 2018.

[14] Nathan Thornburgh, 'The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),' *Time*, September 5, 2005.

[15] Nicholas Schmidle, 'The Digital Vigilantes Who Hack Back,' *The New Yorker*, April 30, 2018.

[16] Jaikumar Vijayan, 'Reverse hacker wins $4.3M in suit against Sandia Labs,' ComputerWorld, February 14, 2007.

[17] Nicholas Schmidle, 'The Digital Vigilantes Who Hack Back,' *The New Yorker*, April 30, 2018.

operation gone right. Meaning, hacking back does work within certain perimeters against certain threat actors. But does it also work again others?

Taxonomy of hacking back operations

Taking the three historical cases, we can distinguish between three categories of hacking back operations that fulfil the aspects of being (a) aggressive and (b) playing by different rules than classical network defenders do: (1) pre-emptive hacking back operations (i.e., before an adversary launches its activity – ex. Max Butler case), (2) reactive hacking back operations (i.e., during an adversary's active operation – ex. Cliff Stoll case), and (3) retributive hacking back operations (i.e., after an adversary has achieved its operational goal – ex. Shawn Carpenter case). Within these three stages we can also distinguish between various degrees of operational intensity.

Pre-emptive hacking back operations are indistinguishable from pre-emptive hacking operations. Meaning, they are part of a chain of potential events that might kick off if pre-emptive action is not taken. Three recent examples can help us separate the degrees of operational intensity.[18] Situated at the lowest end, is the action taken by an actor known as HackerGiraffe who exploited an open network port to print out 'subscribe to Pewdiepie' messages on hundreds of thousands of printers across the globe in late-2018. As HackerGiraffe put it back then, "your printer is exposed. I'm trying to warn you to close it, how else am I gonna get your attention?"[19] Other than costing a few sheets of paper and a bit of printer ink, HackerGiraffe's actions were widely perceived as an efficient – although illegal – way to gain user attention to close their ports. In the mid-range of intensity, is the case of a Russian server administrator known only as Alexey, who broke into over 100.000 MikroTik routers during the months of April to October 2018. The vulnerability Alexey exploited was a 0-day discovered back in March, whose patch was made readily available in April.[20] Given that few users would patch their low-cost routers, Alexey decided to take unilateral action by accessing the vulnerable/infected devices and added "a firewall rule that blocked access to the router from outside the local network."[21] As Alexey put it, "from May to today, I 'wrenched' more than 100 thousand MikroTik devices from the clutches of the botnet." Despite Alexey's good intentions, his actions are still considered unlawful and did not receive much attention nor praise from the infosec community.

On the high-end in terms of aggressiveness, is the case of a hacker known only as The Janit0r, the alleged creator of the BrickerBot malware. Brickerbot's purpose was to literally clean the internet of unsecure IoT and network devices by intentionally overwriting their flash storage/firmware with random data – leaving them unusable in the process (i.e., bricked). In his personal mission against the spread of IoT botnets, the

[18] Granted the mass exploitation of IoT devices is not the same as identifying and breaching specific C&C servers, but the concept of pre-emptively exploiting vulnerabilities to secure or take-out infrastructure assets is nonetheless the same.

[19] Patricia Hernandez, 'Someone hacked printers worldwide, urging people to subscribe to PewDiePie,' *The Verge*, November 30, 2018.

[20] Catalin Cimpanu, 'MikroTik patches Zero-Day flaw under attack in record time,' *BleepingComputer*, April 24, 2018.

[21] Alexey, 'Why hackers Mikrotik and how I hid 100 thousand. RouterOS from botnet,' *Sudonull*, n.d.

Janit0r claimed to have bricked over two million devices within five months, which even led the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to issue an official alert.[22] In December 2017, the Janit0r announced his retirement by publishing snippets of Brickerbot's source code and a 3000-word manifesto in which he claimed to have bricked over 10 million devices all in all.[23] Writing in January 2018, Justin Shattuck, Principal Threat Researcher at F5 Labs, called the Janit0r's ethics "unquestionably wrong," noting that "however 'noble' the intention might be, obtaining unauthorized access to devices and making them unusable, whether temporarily or permanently, is still illegal, and it undermines the work of ethical researchers."[24]

While I do understand Shattuck's sentiment, I would argue that the actions of HackerGiraffe, Alexey, and the Janit0r, should not be seen as vigilantism, but viewed as pre-emptive attack vectors to pro-actively tackle the growth, spread, and status quo of adversarial infrastructure - including phishing sites, proxy servers etc.[25] Granted, their actions are ethically questionable and most likely will never be deemed lawful, but they do provide a practical alternative to achieve success in an area where the infosec community has been struggling - if not even continuously failed – since the birth of internet.

Reactive hacking back operations are most likely rather rare, as most of these occurrences are either mitigated by immediately ejecting an intruder from the network upon discovery or tracking him inside the network to gain forensic evidence and then ejecting him.[26] For the overwhelming majority of companies the overarching premise is not to hunt down adversaries within their own network, but to keep business operations going. As such, attribution and persistently tracking an adversary beyond a defender's own network is not going to produce a discernible return of investment. As Artturi Lehtiö, director for strategy and corporate development at F-Secure, rightly noted, "this isn't a question of offence versus defence. Cybercriminals focus 100 per cent on attacking targets, while companies focus on business and, where possible, cybersecurity protection."[27] Cliff Stoll's case is a tiny bit exceptional in this regard, because (a) Berkeley is not a company, and (b) throughout Cliff's investigation the adversary had access to Berkeley's network – which under normal circumstance no company nor institution would voluntary allow to occur. Similarly, back in the old days, the logic was that "the time to back-hack a perpetrator is within seconds, minutes or hours of the action, not months and years after it happened. The trail is far too cold by then," as John Arquilla explained

[22] CISA, 'ICS Alert (ICS-ALERT-17-102-01A) - BrickerBot Permanent Denial-of-Service Attack (Update A),' US-CERT, April 12, 2017.

[23] Catalin Cimpanu, 'BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices,' *BleepingComputer*, December 11, 2017.

[24] Justin Shattuck, 'BrickerBot: Do "Good Intentions" Justify the Means—or Deliver Meaningful Results?' *F5 Labs*, January 16, 2018.

[25] See for example: https://www.vice.com/en/article/qvvke7/email-provider-protonmail-says-it-hacked-back-then-walks-claim-back; https://twitter.com/notdan/status/1310614849534062592

[26] For an early case on tracking an adversary to gain forensic insights see: J.P. Lawrence, 'Dutch hacker case in early 90s was a test for San Antonio cyber pioneers,' *San Antonio Express News*, August 4, 2017.

[27] Adrian Bridgwater, 'Hacking back: is it a good idea?' *Raconteur*, July 2, 2018.

to PBS in 2003.[28] Cliff was only able to hold the adversary's interest by deploying stacks and stacks of fake government documents on Berkeley's network (nowadays we would call this a rudimental honeypot). In fact, Cliff was told numerous times by his superiors to shut down his investigation and eject the intruder from the network.

Other instances of reactive hacking back are less clear, particularly those touching upon fourth party intelligence collection.[29] FireEye's case is probably the most well-known one, as it was kicked off by revelations in David E. Sanger's 2018 book 'The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.' While Sanger accused Mandiant/FireEye investigators of "reach[ing] back through the network to activate the cameras on the hackers' own laptops [APT1]," FireEye defended its actions by explaining that "all of these videos were made through information obtained via consensual security monitoring on behalf of victim companies that were compromised."[30] It might well be that especially when it comes to fourth or even fifth party intelligence collection, the line between legal and illegal does not formally exist anymore, as standardized practices and their wide-ranging application have erased any pretence of unlawfulness and relation to hacking back.[31] Despite these discrepancies and lack of publicly known cases, reactive operations have nonetheless attracted most of the public discussions on hacking back, painting a picture of concurrent interaction between two parties across both time and space during first contact. I would posit that this is rarely if ever the case because hacking back operations do not move at that speed as they require substantial intelligence collection and a significant level of preparedness on the defender's end. Thus, in the FireEye case, it is highly likely that this was not FireEye's first encounter with APT1, but it might have been the first encounter by the company that FireEye was consensually monitoring.

One interesting case of reactive hacking back occurred in September 1998 when a group of cyber activists and artists known as the 'Electronic Disturbance Theater' (EDT) decided to perform a virtual sit-in – i.e., a DDoS attack - against the Pentagon's defenselink.mil website to protest the war in Mexico. The way it practically worked was through a simple web-based Java applet called FloodNet, which would redirect users to a target website and then constantly reload the target website every few seconds. If enough people participated in the campaign, they would slow down and eventually crash the target. And here the story forks. The most widely spread – and false – narrative is that the Pentagon prepared for the EDT's onslaught by redirecting the incoming requests to its own Java applet dubbed 'hostileapplet.' According to Ricardo Dominguez – founder of the EDT – the Pentagon's applet caused a "series of rapidly appearing Java coffee cups across the bottom of the browser screen coupled with the phrase 'ACK.'" [32] Eventually crashing the attacking browsers. In the aftermath of the incident, several

[28] PBS, 'Cyber War!' *Frontline*, April 24, 2003.

[29] Juan Andres Guerrero-Saade & Costin Raiu, 'Walking in your Enemy's Shadow: When Fourth-Party Collection becomes Attribution Hell.' Kaspersky, March 2018.

[30] FireEye, 'Doing our Part – Without Hacking Back,' *FireEye*, June 25, 2018.

[31] Robert M. Lee, 'Not trying to be pedantic with you; I'm noting that Mandiant in this case wasn't doing anything fancy or cool it did something that ought to be illegal,' Twitter, June 23, 2018.

[32] Robert Wildt, 'Should You Counter-Attack when Network Attackers Strike?' Global Information Assurance Certification Paper, SANS Institute, p. 2.

pundits and infosec professionals claimed that the Pentagon's actions had not only broken numerous domestic laws but even violated the 1878 Posse Comitatus Act.[33]

The other – and true – narrative is slightly different. Accord to an FBI document FOIA'd by security researcher Cian Heasley, the DoD's Defense Technical Information Center (DTIC) wrote a Perl script that "redirected any malicious traffic away from DefenseLINK to a non-existent site" in an attempt to "filter out the denial of service attempts and still provide service to legitimate users." The FBI concluded that "when the EDT protestors continually sent request messages to the search engine, the protestors should have received an error message pop-up, advising that the DefenseLINK website could not be found. If the protestors launched multiple attacks, then with every attempt to shut down DefenseLINK, the protestors would get another error message back. As a result, with all of these error messages coming back, the protestor would be forced to reboot the machine."[34] On November 10, 1998, the Eastern District of Virginia declined to prosecute anyone at DTIC, and the case was closed. The Pentagon never publicly explained what happened – most likely hoping that the incident and EDT would be forgotten over time. Given that the Pentagon's actions did achieve – although unintended – a discernible impact on the attacker's end, would we - by today's standards - consider the incident to fall into some kind of "passive" reactive hacking back tactic? You decide.

By contrast, retributive operations are probably the most common form of hacking back. Talking to the Daily Beast in 2017, former FBI agent E.J. Hilbert for example stated that he knew five companies that hacked back – two government contractors, two in the retail sector, and the fifth was a manufacturing firm. According to Hilbert, "all five companies retaliated to try and understand what exactly hackers managed to steal during a breach. But all the companies had trouble locating the system the hackers used to transmit the data in the first place."[35] At the lower end of this spectrum are operations that are purely conducted for reconnaissance purposes, i.e., finding and accessing adversarial boxes or even breaching networks in the adversary's proximity. This can include anything from baiting a target into downloading a malicious file on a honeypot – as done by the Georgian government CERT in late-2012, who used their access to take webcam pictures of an alleged Russian-based hacker who was running a month-long espionage campaign against the Caucasus nation.[36] To outright targeting and breaching a network within a specific geo-tagged building – as conducted by the Netherlands' domestic intelligence service in 2014 to penetrate and surveil a hacking team run by Russia's Foreign Intelligence Service (SVR).[37] In the mid-range of aggression are operations that crash and burn adversarial boxes by, among other things, deleting or encrypting their content. US Cyber Command's Joint Task Force ARES for example used this method in

[33] Winn Schwartau, 'Can you counter-attack hackers?' *CNN*, April 7, 2000.

[34] Cian Heasley, 'FBI FOIA Response sheds new light on infamous hacktivist Pentagon incident,' *Medium*, October 27, 2020.

[35] Joseph Cox, 'Revenge Hacking Is Hitting the Big Time,' *The Daily Beast*, September 19, 2017.

[36] Nate Anderson, 'How Georgia doxed a Russian hacker (and why it matters),' *ArsTechnica*, November 2, 2012.

[37] Huib Modderkolk, 'Dutch agencies provide crucial intel about Russia's interference in US elections,' *Volkskrant*, January 25, 2018.

their coordinated campaign against the Islamic State in 2016.[38] At the high-end are those operations that are waged on a purely personal level. Two known cases stand out in that context: Blue Security in 2006 and HBGary in 2011.

Based in Herzlia, Israel, Blue Security was a novel anti-spam company created in 2005 that offered a community-based software solution that would send out massive amounts of "automated opt-out requests on behalf of its registered users to companies whose products are advertised by spammers."[39] At its height, Blue Security encompassed more than 522.000 active users.[40] In April 2006, its userbase was aggressively spammed in an attempt to intimidate its members to drop out of Blue Security's network. Following that initial campaign, a massive DDoS attack was run against Blue Security's website, and the adversary also succeeded in bribing a staffer at a large ISP into black holing Blue Security's IP address – rendering it inaccessible outside of Israel. When Blue Security reappointed its domain to a TypePad-hosted blog run by Six Apart – one of the largest blog networks at the time - the adversary DDoS'd the blog and also brought down Six Apart in the process for its millions of users. If that were not enough, Blue Security's domain name service provider Tucows was additionally hit with a massive DDoS and knocked offline for several hours, making thousands of websites unreachable.[41] Tucows chief executive Elliot Noss called the attack "by far the largest the company had ever seen."[42] The campaign also "disrupted the net operations of five top-tier hosting providers in the US and Canada, as well as a major DNS provider for several hours." Behind it all, a Russian spammer known as PharmaMaster, who acknowledged in a conversation with the Register that "if he can't send spam, there will be no internet."[43]

Given the onslaught and personal nature of the campaign, Blue Security concluded that they would be unable to safely reintroduce their service without exposing other members of the internet community to another attack. Talking to the Washington Post, CEO and founder of Blue Security Eran Reshef stated that "it's clear to us that [quitting] would be the only thing to prevent a full-scale cyber-war that we just don't have the authority to start. Our users never signed up for this kind of thing."[44] John Leyden over at the Register summarized the outcome aptly by stating that, "Blue's decision to shut up shop is understandable but regrettable, because it represents a significant victory by a spammer in the fight to control the internet. In effect, PharmaMaster has succeeded in his main aim of getting Blue Security to dismantle."[45]

[38] Dina Temple-Raston, 'How the U.S. hacked ISIS,' *NPR*, September 26, 2019.

[39] Wired Staff, 'I'm the Blue Security Spammer,' *Wired*, May 5, 2006.

[40] Brian Krebs, 'In the Fight Against Spam E-Mail, Goliath Wins Again,' *The Washington Post*, May 17, 2006.

[41] Gregg Keizer, 'Blue Security Gives Up, Spammer Wins,' *CRN*, May 17, 2006.

[42] Brian Krebs, 'In the Fight Against Spam E-Mail, Goliath Wins Again,' *The Washington Post*, May 17, 2006.

[43] John Leyden, 'Blue Security calls it quits after attack by renegade spammer,' *The Register*, May 17, 2006.

[44] Brian Krebs, 'In the Fight Against Spam E-Mail, Goliath Wins Again,' *The Washington Post*, May 17, 2006.

[45] John Leyden, 'Blue Security calls it quits after attack by renegade spammer,' *The Register*, May 17, 2006.

The second case is the rather embarrassing story of security firm HBGary, which is probably also the craziest publicly known retributive hacking back operation known to date. Everything started with Aaron Barr, then CEO of HBGary Federal, and his publicity hungry claim that he penetrated the loose hacker collective Anonymous and was able to identify their ringleaders solely based on social media data and subterfuge. When Barr's claims were picked up by the Financial Times on February 4, 2011, whose story also announced that Barr would release his findings at a security conference in the same month, it grabbed the interest and anger of Anonymous.[46] On February 5, HBGary Federal was DDoS'd, its website defaced, and Anonymous gained access to the internal email server, extracting more than 40,000 emails and releasing them on Pirate Bay for all to see. Anonymous also took over Barr's Twitter and LinkedIn accounts, and published Barr's social security number and home address.[47] In an after-action IRC chat, Anonymous members also bragged about deleting 1TB of HBGary Federal's backup data and claimed to have wiped Barr's iPad remotely.[48]

If this were not enough, Anonymous also ran a social engineering campaign against Greg Hoglund owner of HBGary (the parent company that partially owned HBGary Federal) who operated rootkit.com. With information snippets in the breached emails Anonymous successfully engineered its way to gain root access on rootkit.com. They defaced the website, dumped the user database and even cracked all the user passwords.[49] Nate Anderson over at ArsTechnica published a detailed background story as to why Barr did what he did and the subsequent fallout HBGary had to deal with. As Nate beautifully summarized, "The attackers are quintessentially Anonymous: young, technically sophisticated, brash, and crassly juvenile, all at the same time. [..] Perhaps the entire strange story can be best summed up by a single picture, one that Barr e-mailed to two of his colleagues back on January 28. 'Oh fuck,' it says beneath a picture of an Anonymous real-world protest. 'The Internet is here.'[50]

Conclusions

So, what do these two cases tell us? First, making it personal is a really bad idea because once emotions are involved anything can happen. Which is also a neat way to distinguish between individuals and lose groups on the one hand, and more hierarchical organizations (think large cybercriminal groups and APTs) that have a leadership in place to temper quick and emotional decision making. Roughly speaking, this might indicate a reference point as to who to avoid when hacking back, and which entities are less likely to run up the escalation ladder. Second, the absence of many more public cases that fall into this category might indicate that this problem is not as widespread as

[46] Nate Anderson, 'How one man tracked down Anonymous—and paid a heavy price,' *ArsTechnica*, February 10, 2011.

[47] Jacqui Cheng, 'Anonymous to security firm working with FBI: "You've angered the hive",' *ArsTechnica*, February 7, 2011.

[48] Nate Anderson, 'How one man tracked down Anonymous—and paid a heavy price,' *ArsTechnica*, February 10, 2011.

[49] *Ars Staff*, 'Anonymous speaks: the inside story of the HBGary hack,' ArsTechnica, February 16, 2011.

[50] *Nate Anderson*, 'How one man tracked down Anonymous—and paid a heavy price,' ArsTechnica, February 10, 2011.

we think it is. If an emotional actor lashes out it in the way that Anonymous and PharmaMaster did, the blast radius will probably not go unnoticed within the infosec community. Then again, it could also be that many similar stories were never written up or are still kept secret within parts of the community.

Having gone through all of these disparate cases, what I am hopefully leaving you with is a more refined understanding of the different kind of hacking back operations we are dealing with. Should companies conduct pre-emptive hacking back? Maybe they should. Should companies conduct reactive hacking back? They likely do not and cannot. Should companies conduct retaliatory hacking back? Against hierarchically organized rational actors, probably yes. Against individuals and smaller groups, preferably no.

In sum, I partially agree with Sanija Ameti and Fabian Reinhard, but for very different reasons. To me, the subject of hacking back is much more complex and nuanced to the extent that it should not be legislated in any way shape or form. If companies want to hack back, they should do so on their volition and risk no matter their underlying motivations. Not everything in cyberspace has to be legislated to make sense and have meaning. And not everything has to have a meaning and make sense in cyberspace.