CYBERDETERRENCE AND THE PROBLEM OF ATTRIBUTION

A thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirement for the
degree of
Master of Arts
in Security Studies

By

Ryan Richard Gelinas, B.S.

Washington, DC
April 16, 2010

TABLE OF CONTENTS

Introduction	1
Deterrence	3
Cyber Attacks and Attribution – Case Study	6
Estonian Cyber War	6
Moonlight Maze	10
Brazilian Power Outages	12
Aurora	15
Titan Rain	19
Lessons for Attribution	21
Conclusion - Implications for Deterrence	24
Bibliography	26

INTRODUCTION

The computer networks of the United States, including defense, government, and commercial sectors, are under constant attack and even more frequent probing. Ranging from denial of service attacks to backdoor-implanting espionage to attempts to bring down critical infrastructure, these computer network attacks fill a spectrum from juvenile on one end to dire on the other. Having failed to field an effective comprehensive computer network defense strategy, some have suggested that the U.S. establish a doctrine of cyber-deterrence as a core component of such a strategy. Determining the feasibility of cyberdeterrence is of critical importance as the U.S. prepares to establish a new military command, U.S. Cyber Command, which would be responsible for carrying out such a doctrine. This doctrine would vow proportional and measured cyber attacks against nations attacking U.S. network infrastructure in order to deter attacks from taking place.[1] However, cyber warfare, unlike the nuclear warfare dynamic that gave birth to our contemporary understanding of deterrence, is dissimilar in ways that make deterrence a difficult policy and a broader deterrence strategy one potentially destined to fail.

The core problem of cyber warfare is the problem of attribution. Cyber attacks are not easily attributed. Attackers can hide in the cloud. Determined combatants can disguise themselves as other actors. Conducted properly, the victim never knows the attack is occurring and may be lucky to discover it years after the fact. Complicating this further, attacks directed by states need not be conducted by states. Some victims, presented with evidence of attribution, may not wish to acknowledge attacks for political reasons. In analyzing a series of significant

[1] Alexander, Keith. "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command." Senate Armed Services Committee. 14 April 2010. (http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf). 15 April 2010.

contemporary cases of cyber attacks, I will show that attribution at a degree required by a deterrence policy is so difficult that a deterrence strategy is *ipso facto* infeasible.

DETERRENCE

Deterrence strategy is a framework under which the deterring state, under threat of pain, demands that the deterred state does *not* conduct a specific, overt action. Deterrence is fundamentally about the maintenance of the status quo on the part of the deterring state, designed to maintain a specific condition under threat of change by the deterred party. The setting of demands by the deterring state is generally non-provocative—it consists of, as Thomas Schelling explains, *setting the stage* and *waiting*; in contrast, overt actions on the part of the deterred state to violate those demands are viewed as provocative.[2] Primary to the value of deterrence is the realization that violence is best utilized when it is threatened but not used, as Schelling identifies.[3] This contrasts with the employment of brute force.

The mechanics of deterrence have been likened to a "trip wire" or "plate-glass window," as Schelling identifies in his discussion of U.S. troops in Berlin as an empirical example.[4] In this situation, the deterrence calculus identifies the troops as a "trip wire" that, if attacked by the Soviets or their satellites, would trigger a massive military response on the part of NATO. To increase the robustness of the deterrent threat, a deterrent state can engage in a *commitment process* under which it eliminates possible situations that may give it avenues to avoid enforcing its deterrence strategy demands upon the deterred state, all in an attempt to make the deterrent threat more credible.[5] Schelling uses the example of Quemoy, but perhaps a better example would be the "doomsday machine" from the nuclear deterrence satire *Dr. Strangelove*. By automating the processes of this machine so that no human could interrupt and prevent universal global atomic holocaust in the event of an attack on the Soviet Union, the Soviets had achieved

[2] Schelling, Thomas. Arms and Influence. New Haven: Yale University Press, 1966. Pages 71-72
[3] *Ibid*., Page 10
[4] *Ibid*., Page 47
[5] *Ibid*., Page 44

the perfect deterrent by *committing* themselves to mandatory enforcement of their threat. Of course, this highlights an obvious issue with deterrence in general, that the deterrent threat has to be *communicated* to the enemy and properly understood; an unknown or misinterpreted deterrent is not a deterrent.

Deterrence is not without its shortcomings. One well-discussed impediment to effective deterrence is the utilization of *salami tactics*, an attempt by the deterred state to progressively and in small steps come close to and or actually violate the demands of the deterring state in a way that prevents the deterrent from being employed.[6] A recent example of salami tactics can be seen in the 2006 conflict between Hezbollah and Israel. While Israel made clear to Hezbollah that it would not tolerate rocket fire on its population centers and the kidnapping of its soldiers, Hezbollah periodically did both, growing bolder with each operation. The Israeli deterrent was not used after the first harassing Hezbollah events, reducing its power and credibility. Hassan Nasrallah stated as such when Israel finally invaded in July 2006 after another provocation; he had no expectation of an Israeli response[7], showing that he had no faith in Israel's threat. As Schelling identified, to be effective the threat has to be credible.[8] The deterring party has to threaten that it *will* act to prove its commitment; *may* act is not sufficient.[9]

Absent from much of the Cold War deterrence literature is the discussion of attribution. Most writers during this period examined deterrence in the U.S.-Russia framework. Attacks, be they conventional or nuclear, were always assumed to be attributable. Either the U.S. launched ballistic missiles first or the Soviets did. There were no immediate concerns that rogue,

[6] *Ibid*., Page 66
[7] Noe, Nicholas, ed., Voice of Hezbollah: the Statements of Sayyed Hassan Nasrallah. London: Verso, 2007

[8] Schelling, Thomas. The Strategy of Conflict. New York: Oxford University Press, 1960. Page 6
[9] *Ibid*., Page 187

unattributed ICBMs would start raining down upon America. Attribution was so integral to the analysis of deterrence as a strategy that it was hardly worth a mention.

This issue of attribution, so clear in the Cold War context, becomes muddy and complex when applied to the realm of cyber warfare. Take a simple policy statement, for example: the United States will respond with a massive cyber-offensive against China and its interests in the event of a Chinese attack on the United States or its interests, sufficient in scale as to deter China from conducting such an attack. Chinese long-range bombers would be detectable flying over the Pacific, as would ICBMs as they hurtle through space towards San Francisco. But packets streaming through an undersea fiber optic cable landing at a terrestrial fiber backbone switching center in Los Angeles, destined to cripple American defenses, power production, or early-warning radar, would in all likelihood be undetectable. At that moment a prospective American cyber-deterrence strategy would be impotent. Deaf, dumb, and blind, the U.S. government would know it had been attacked—but by whom? Who would the U.S. strike back against in righteous anger?

CYBER ATTACKS AND ATTRIBUTION – CASE STUDY

To illustrate the problem of attribution, I will analyze five contemporary "cyber attacks," broadly defined. This basket of cases will include attacks against both government and civilian infrastructure as well as a variety of attack methods ranging from denial of service attacks to potentially crippling sabotage of critical infrastructure. In each case I will explore a series of questions:

- Who attributed the attack?
- At what confidence was the attack attributed?
- How was the attack attributed?
- How long of a delay was there between attack and attribution?
- What was the response of the attack's victim?

This set of cases will show the difficulties of attribution of cyber attacks, especially highlighting the uncomfortably circumstantial nature of cyber-attribution. Throughout these cases, attribution will be shown often to be technically infeasible, politically undesirable, and in some cases, both. Due to the lack of published reports of cyber warfare, several of the cases I examine will not be especially consequential, particularly when presented to a U.S. audience. The cases available for analysis are few, and those that exist are poorly sourced. But the lessons learned in these cases I examine are universal, no matter how trivial or significant the consequences of the attacks.

ESTONIAN CYBER WAR

On 27 April 2007, the Estonian government relocated a Soviet-era World War II memorial. A lightning rod for the acrimonious division between ethnic Russian and Estonian

nationalist elements with Estonian society, its relocation triggered violence on the streets.[10] To many Estonians and the Estonian government, the memorial was a reminder of Soviet occupation and oppression, while to pro-Russian elements it memorialized those who fought valiantly against the Nazis. The move caught the attention of Russian President Vladimir Putin, who condemned the move.[11]

Estonia is more wired and utilizes the internet more than most countries. Online banking is extensive and in 2007 a fraction of the votes for parliament were conducted online.[12] As a result of Estonia's greater cyber linkages, cyber attacks would have had a significant negative impact.

A few days before it began, Estonia realized that a cyber attack was coming. Postings on Russian-language web forums suggested that a major cyber effort was underway.[13] Estonia refrained from publicly warning Russia as diplomatic efforts were underway to defuse the crisis. On 26 April 2007 at 10:00 p.m. local time, distributed denial of service attacks began against a list of Estonian websites.[14] Step-by-step instructions allowed any internet user to launch attacks of their own.[15] Public websites and mail servers for a variety of organizations suffered and began crashing. Supplementing manual efforts, unknown attack coordinators triggered botnets to begin attacking Estonia, drastically increasing the stream of packets targeting Estonian

[10] "Estonia Blames Russia for Unrest." BBC News. 29 April 2007. (http://news.bbc.co.uk/2/hi/europe/6604647.stm). 15 February 2010.
[11] *Ibid*.
[12] Evron, Gadi. "Battling Botnets and Online Mobs." Georgetown Journal of International Affairs. Winter/Spring 2008:122.
[13] *Ibid*.
[14] *Ibid.*
[15] Hypponen, Mikko. "9th of May." F-Secure Weblog. F-Secure. 9 May 2007. (http://www.f-secure.com/weblog/archives/archive-052007.html). 15 February 2010.

infrastructure.[16] Websites were defaced and services stopped. The onslaught continued for over three weeks while Russian authorities did nothing to stop or discourage the attacks. Attacks peaked on 9 May, which was Victory Day in Russia.[17] The political damage outweighed the actual damage caused by the attacks; slowing internet connections, taking down websites, and defacing others were more of a nuisance than a threat.

On 17 May Estonian Foreign Minister Urmas Paet directly blamed the Russian government for direct involvement in the attacks, which he claimed targed Estonian government websites, telephone networks, and emergency response systems.[18] He also directly attributed the attacks to Russian government infrastructure, claiming that they came from IP addresses and servers assigned to the Russian government.[19] Though appealing for help against a perceived Russian government onslaught, Estonian defense minister Jaak Aaviksoo admitted that NATO's collective defense Article V could not be invoked because "not a single NATO defense minister would define a cyber-attack as a clear military action at present."[20] The Estonian defense ministry hinted that, in addition to blocking access to Estonian infrastructure from foreign IP addresses, "people" started to fight against the cyber attack, claiming that "ways were found to eliminate the attacker."[21]

Other knowledgeable analysts cast doubts on the veracity of Paet's claim. Mikko Hypponen, chief research officer at computer security firm F-Secure, pointed out that Russian

---

[16] Evron, Gadi. "Battling Botnets and Online Mobs." Georgetown Journal of International Affairs. Winter/Spring 2008:123,
[17] Hypponen, Mikko. "9th of May." F-Secure Weblog. F-Secure. 9 May 2007. (http://www.f-secure.com/weblog/archives/archive-052007.html). 15 February 2010.
[18] Halpin, Tony. "Estonia Accuses Russia of 'Waging Cyber War.'" Times Online, 17 May 2009. (http://www.timesonline.co.uk/tol/news/world/europe/article1802959.ece). 15 February 2010.
[19] *Ibid*.
[20] Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." The Guardian. 17 May 2007. (http://www.guardian.co.uk/world/2007/may/17/topstories3.russia). 15 February 2010.
[21] *Ibid.*

government computers may have been infected by the botnet used to launch denial of service attacks.[22] Additionally, even if the attacks were overt, they just as easily could have been committed by anyone, "from the son of some ministerial janitor upwards."[23] Hypponen and others have also claimed that a true Russian government attack would have been far stronger and lasted much longer, with the results more devastatingly crippling for Estonia. This assumes that the Russian government wanted to be identified as the culprit; in a cyber war, measured attacks by proxy deflect blame and attribution when both are unwanted.

Interestingly, nearly two years later, a member of the Russian Duma, Sergei Markov, explained a possible government hand in the attacks. He claimed that an unnamed assistant of his coordinated the attacks while residing in one of Russia's "unrecognized republics," possibly Transnistria.[24] While not explicitly coordinated by the Russian government, Markov admitted that there was passive government support to what he described as "purely a reaction from civil society" out of a sentiment that "something bad had to be done to these fascists."[25]

Markov's assessment of the situation is the most plausible in retrospect: patriotic Russian hackers, with support of individuals acting in a non-governmental capacity but with passive encouragement from elements of the Russian government, banded together to attack with criminally-sourced tools like Trojans and botnets. Not criminal, not state-driven, not nationalists, not pranksters, but rather a mix of them all were responsible for what has been

[22] Rantanen, Miska. "Virtual Harassment, but for Real." Helsingin Sanomat. 6 May 2007. (http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868). 15 February 2010.
[23] *Ibid.*
[24] Coalson, Robert. "Behind the Estonia Cyberattacks." Radio Free Europe / Radio Liberty. 6 March 2009. (http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html). 15 February 2010.
[25] *Ibid.*

termed a "cyber riot" rather than a cyber attack.[26] While information released by the Estonians and analysis by independent investigators suggested this was the case, it was not until this moment 23 months later that attribution was this clear. Future victims of cyber attacks, however, cannot rely on the attacker claiming victory as the default method of attribution.

MOONLIGHT MAZE

Long before cyber warfare gained an elevated status and before a Department of Defense cyber command was a possibility, the Moonlight Maze intrusion set rattled the U.S. defense establishment. In March 1998, back in a time when cyber warfare was referred to as "netwar," the U.S. government detected broad intrusions into defense networks, NASA, and other government agencies. These intrusions, purported to be coming from Russia, were termed Moonlight Maze by the intelligence community.

James Adams, chairman of a cybersecurity firm and a member of the National Security Agency Advisory Board, made a splash in May 2001 when he announced the intelligence community's Moonlight Maze investigation in Foreign Affairs.[27] Expanding upon the Government Accountability Office's brief mention of Moonlight Maze earlier that year, Adams claimed that for three years the U.S. government was investigating actions by a "group of hackers" targeting the Department of Defense, NASA, private universities, research labs, and government agencies.[28] [29] Others specifically identified the Department of Defense's unclassified NIPRNET system as the biggest target.[30]

---

[26] James Hendler, as cited in Waterman, Shaun. "Analysis: Who Cyber Smacked Estonia?" United Press International. 11 June 2007. (http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/). 15 February 2010.
[27] Adams, James. "Virtual Defense." Foreign Affairs. May/June 2001.
[28] "Information Security: Challenges to Improving DOD's Incident Response Capabilities." U.S. General Accounting Office. March 2001. (http://www.gao.gov/new.items/d01341.pdf). 15 February 2010.

These hackers were claimed to have targeted information stored on those systems, including contract details, encryption techniques, and sensitive but unclassified defense information.[31] Covert backdoor tools were installed and specific network traffic was routed to Russian servers. Adams hinted that the grounds for future sabotage were laid and that many more questions were left unresolved. Adams claims that the attacks appeared to come from Russian-registered IP addresses, but no definitive links to a state-sponsored effort could be found. Dion Stempfley, a former analyst at the Pentagon who helped detect Moonlight Maze, suggested that the attacks were "state allowed," in that the Russian government was either directing or knowingly permitting the attacks.[32] Attempts to "hack-back" were limited because the Pentagon was fearful of conducting an act of war in the even the attacks were coming from a state program.[33] The Russian government was demarched on the issue and pleaded ignorance in the face of evidence.

Moonlight Maze was one of the first true cyber incidents to target the U.S. defense establishment. No information has been made public regarding the timeline of attribution. First detected in March 1998 by computer network analysts at the Department of Defense, Moonlight Maze may have been going on for years without detection. Even after detection, years of analysis were required to understand and roughly attribute Moonlight Maze to Russian actors. Even with the best resources of the U.S. government marshaled to analyze the attacks and intrusions, no conclusive links could be found to the Russian government or another large, deterrable actor. The frustrating lessons of Moonlight Maze persist; its story has been replayed many times in the intervening years as shadowy attackers hiding their tracks have penetrated key

[29] Adams, James. "Virtual Defense." Foreign Affairs. May/June 2001.
[30] Loeb, Vernon. "Pentagon Computers Under Assault." Washington Post. 7 May 2001: A02.
[31] Adams, James. "Virtual Defense." Foreign Affairs. May/June 2001.
[32] Loeb, Vernon. "Pentagon Computers Under Assault." Washington Post. 7 May 2001: A02.
[33] *Ibid.*

U.S. government systems only to see the U.S. passively monitor and improve defenses. Moonlight Maze gave the U.S. its first taste of the problem of attribution and the other cases analyzed here illustrate how the problem is a persistent one.

BRAZILIAN POWER OUTAGES

Possible cyber attacks against power infrastructure in Brazil in 2005 and 2007 may have caused millions of people to lose power and plunged cities into darkness. The operative word here is *possible*; these could have either been two of the most devastating cyber attacks of all time, with the greatest immediate real-world implications, or they may not have been cyber attacks at all. Alarmingly, these two cases illustrate both the potential of cyber attacks to do real harm as well as the tangled web of attribution. While sourcing of details related to these possible attacks is tenuous at best, available information can provide valuable lessons.

U.S. security and intelligence officials have publicly painted a broad story in which an unnamed country had cities that suffered cyber attacks that "plunged entire cities into darkness."[34] Tied to off-the-record statements from similar officials, CBS News claimed in November 2009 that a number of credible sources indicated that cyber attacks were responsible for two power outages in Brazil. The first occurred north of Rio de Janeiro in January 2005, cutting power to three cities and leaving tens of thousands without power.[35] The second and most severe occurred on 26 September 2007 in the state of Espirito Santo, cutting power to more than three million people, dozens of cities, and a network of plants belonging to an iron ore

[34] Messick, Graham. "Cyber War: Sabotaging the System." CBS News. 8 November 2009. (http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml). 15 February 2010.
[35] *Ibid.*

producer.[36] Their claim, which was rolled into a larger alarmist report on cyber warfare, did not attribute the attacks nor did it provide a motive. Tied to this incident are statements by CIA cyber official Tom Donahue, who claimed that the U.S. government had information indicating that in "at least one case" cyber attacks led to the disruption of power in multiple cities and that the government had seen multiple examples of cyber intrusions followed by extortion demands.[37] The CBS report as well as former Bush administration official Richard Clarke explain that this unnamed victim was Brazil.[38] [39]

Brazilian officials not only deny that the cyber attacks took place but offer a specific reason why the blackouts occurred, claiming that physical infrastructure problems unrelated to cyber infrastructure plunged parts of the country into darkness. In the case of the reported 2007 attack, the power company, Furnas Centrais Elétricas, claimed no knowledge of hackers accessing their systems.[40] They explained following the event that the outages were a result of soot and dust accumulating on insulators on high-voltage lines.[41] Months without rain, combined with burning fields emitting large quantities of particulate matter, resulted in dirty insulators that failed to operate properly. Other authorities within Brazil concurred with this explanation, blaming polluted insulators and fining Furnas $3.27 million for failing to maintain its transmission towers properly.[42]

---

[36] Messick, Graham. "Cyber War: Sabotaging the System." CBS News. 8 November 2009. (http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml). 15 February 2010.
[37] "CIA Confirms Cyber Attack Caused Multi-City Power Outage." SANS News Bites. SANS. 18 January 2008. (http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5). 15 February 2010.
[38] Messick, Graham. "Cyber War: Sabotaging the System." CBS News. 8 November 2009. (http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml). 15 February 2010.
[39] Zetter, Kim. "Feds' Smart Grid Race Leaves Cybersecurity in the Dust." Threat Level. Wired. 28 October 2009. (http://www.wired.com/threatlevel/2009/10/smartgrid/). 15 February 2010.
[40] Soares, Marcelo. "Brazilian Blackout Traced to Sooty Insulators, Not Hacker." Threat Level. Wired. 9 November 2009. (http://www.wired.com/threatlevel/2009/11/brazil_blackout/). 15 February 2010.
[41] *Ibid.*
[42] *Ibid.*

Brazil has had a series of failures in its power distribution and generation systems. Just days after the CBS report aired, crippling power outages left over 60 million without power and severely impacted the most populous areas of Brazil as well as all of Paraguay. The blame in this case was assigned to the Itaipu hydroelectric dam, which provides 20% of Brazil's electricity and 90% of Paraguay's.[43]

The Brazilian cyber or non-cyber case illustrates a new range of issues for attribution. Chastened commercial infrastructure providers, even in the face of facts, may seek to avoid blaming failures on cyber attacks. Acknowledging cyber weakness invites more attacks, and, especially if there are no easy immediate fixes, may lead to costly reforms to improve network security. Particularly embarrassing are incidents where cyber attacks benefit from insider knowledge, as Donahue hinted at in his discussion of critical infrastructure vulnerabilities.[44] Blaming the weather or a dirty insulator may be more politically and commercially appealing.

Even if cyber attacks are properly attributed, the victim may not want to advertise the fact. This is not just a problem in the commercial sector, but one for government as well. The U.S. government rarely discloses penetrations of its systems by the Chinese and Russians; only once in a while do specific cases like Titan Rain and Moonlight Maze go public. Public attribution also informs the attacker that the victim is able to detect and discover attack attempts. Particularly for stealthy state-based intelligence gathering and covert cyber operations, victims potentially have far more to learn by identifying attack signatures and quietly studying them to learn attacker methodology, behavior, priorities, and tools. Honeypots, or systems designed to intentionally lure attackers as a way of learning about them, are particularly useful in these cases.

[43] "Major Power Failures Hit Brazil." BBC News. 11 November 2009. (http://news.bbc.co.uk/2/hi/americas/8353878.stm) 15 February 2009.
[44] Zetter, Kim. "Feds' Smart Grid Race Leaves Cybersecurity in the Dust." Threat Level. Wired. 28 October 2009. (http://www.wired.com/threatlevel/2009/10/smartgrid/). 15 February 2010.

Victims may also with to withhold attribution as it implies a vulnerability or weakness that they are unwilling to declare to their domestic constituents.

AURORA

Aurora is the codename given by American computer security firm McAfee to wide-ranging and alarming cyber attacks by China against dozens of American companies starting in December 2009. "Aurora" was allegedly part of the file name of the malware tools on a computer used to attack victims.[45] Brazen in scope and technique, the attacks were a watershed moment for the cybersecurity community, China-U.S. relations, and the future of Google. Most important in the context of this paper, Aurora has eclipsed the murky problem of attribution as multiple entities have either openly or backhandedly blamed the Chinese government for the attacks, with Google going so far as to threaten withdrawing from China altogether in retribution.

The Aurora intrusion set began around mid-December 2009 and lasted until early January 2010, when the redirection servers masking the original attack infrastructure in China were taken down.[46] [47] Attackers lured victims into opening emails or visiting websites embedded with malicious code, a "zero-day" exploit for Microsoft Internet Explorer that allows the attacker to execute malicious code on the target computer.[48] Another attack vector consisted of infected Adobe PDF files embedded with a Trojan called Trojan.Hydraq, which installed on target

[45] Kurtz, George. "Operation 'Aurora' Hit Google, Others." McAfee Security Insights Blog. McAfee Security. 14 January 2010. (http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/). 15 February 2010.
[46] Drummond, David. "A New Approach to China." Google Blog. 12 January 2010. (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html). 14 February 2010.
[47] Zetter, Kim. "Google Hack Attack Was Ultra Sophisticated, New Details Show." Threat Level. Wired. 14 January 2010. (http://www.wired.com/threatlevel/2010/01/operation-aurora/). 15 February 2010.
[48] Kurtz, George. "Operation 'Aurora' Hit Google, Others." McAfee Security Insights Blog. McAfee Security. 14 January 2010. (http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/). 15 February 2010

machines as a Windows DLL file.[49] Triple-encrypted shell code was deployed to target computers, triggering them to download further encrypted binaries which unpacked into two encrypted executable files. These files constituted the backdoor that allowed the computer to talk back to command and control servers, masking communications in encrypted secure socket layer (SSL) connections to best blend in with normal web traffic and avoid proxying and filtering mechanisms.[50] Attackers stole commercial accounts on virtual private servers like Rackspace and Linode, which provide storage and computing solutions in the "cloud," the anonymous server farms that provide virtual servers to match any size and power requirements.[51] These servers and others in Taiwan and the U.S. were used as covert exfiltration pathways for data stolen from target computers. This provided layers of obfuscation for the attackers as in-depth forensics would be required to follow the multiple hops the encrypted data would take back to attacker computers in China.

In addition to being advanced in attack vectors, data exfiltration, and source obfuscation, the Aurora attacks were well-researched and were directed at specific targets with access to key data. The attacks targeted at least 34 different American firms, many of which had operations in China.[52] [53] In all cases, the attackers specifically targeted proprietary intellectual property, specifically source code. In the case of Google, the attackers also targeted Gmail account servers for Chinese human rights activists.[54] To gain access to this data, the attackers not only targeted

---

[49] Zetter, Kim. "Google Hackers Targeted Source Code of More Than 30 Companies." Threat Level. Wired. 13 January 2010. (http://www.wired.com/threatlevel/2010/01/google-hack-attack/). 15 February 2010.
[50] Zetter, Kim. "Google Hack Attack Was Ultra Sophisticated, New Details Show." Threat Level. Wired. 14 January 2010. (http://www.wired.com/threatlevel/2010/01/operation-aurora/). 15 February 2010.
[51] Zetter, Kim. "Google Hackers Targeted Source Code of More Than 30 Companies." Threat Level. Wired. 13 January 2010. (http://www.wired.com/threatlevel/2010/01/google-hack-attack/). 15 February 2010.
[52] *Ibid.*
[53] Zetter, Kim. "Report Details Hacks Targeting Google, Others." Threat Level. Wired. 3 February 2010. (http://www.wired.com/threatlevel/2010/02/apt-hacks/). 15 February 2010.
[54] Drummond, David. "A New Approach to China." Google Blog. 12 January 2010. (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html). 14 February 2010

the people involved but also "swam upstream" by targeting individuals within their targets' social networks. With compromised email or social networking accounts, the ultimate target individuals would have no reason to believe that the friends they talked with were in fact hacked accounts sending attacker malware to key victims.

Adding to the severity and breadth of the attacks, a law firm involved in a U.S. suit against China for stealing proprietary code for unlicensed use in its "Green Dam" domestic internet filtering and censorship software claimed it was the victim of similar attacks.[55] Gipson, Hoffman, & Pancione represents CYBERsitter, a software company that builds internet censoring and filtering software. CYBERsitter had filed a $2.2 billion lawsuit against China for stealing over 3,000 lines of code from its software for use in its Green Dam Youth Escort censorship software. Around the same time as the Google attacks the law firm discovered similar socially engineered attacks against their own employees by hackers seeking access to proprietary court documents.[56]

Multiple parties attributed the Aurora attacks, which were first detected in mid-December and may have begun earlier than that. Security research firm iDefense suggested that the attacks may have been occurring since July 2009.[57] While most attacks hunger for attribution, multiple companies and security firms independently came to similar conclusions about the attacks. Google, McAfee, iDefense, Juniper Networks, Adobe Systems, and Rackspace have all identified themselves as victims of the attacks.

---

[55] Romero, Dennis. "L.A. Law Firm Reports Cyber Attack from China." Los Angeles Weekly. 14 January 2010. (http://blogs.laweekly.com/ladaily/city-news/law-firm-cyber-attack/). 15 February 2010.
[56] *Ibid.*
[57] Zetter, Kim. "Google Hackers Targeted Source Code of More Than 30 Companies." Threat Level. Wired. 13 January 2010. (http://www.wired.com/threatlevel/2010/01/google-hack-attack/). 15 February 2010.

Google publicly called China out in a blog post on 12 January 2010, decrying attacks "originating from China" attacking its corporate infrastructure, stealing intellectual property and targeting human rights activists.[58] Google also conducted its own forensics of the attack, uncovering similar attacks against internet, finance, technology, media, and chemical companies, notifying all of the victims of what it discovered.[59] Some have indicated that Google "hacked back" against the servers engaged in command and control of the attack in order to gain valuable intelligence about the threat.[60] Casting a wide net, Google was able to identify that several users of its email services had their personal computers compromised by attacker malware tied to the Aurora set.[61] Google also linked their experience to other episodes of suspected Chinese state espionage, including the GhostNet global Chinese-origin spying effort targeting pro-Tibet activists around the world that was uncovered by Canadian researchers in 2007.[62] So enraged was Google that it announced it would stop filtering searches on its Chinese internet portal and vowed that it would rather leave China than be forced to infringe on the rights of the Chinese people.

Despite denying any role in the attacks, China has recently taken action in what it claims is an independent investigation into hacking organizations. On 8 February 2010 it shut down the largest hacker training site in China, "Black Hawk Safety Net," and raided its offices.[63] Several people were arrested and servers and cash were confiscated. This followed a public rebuke in

[58] Drummond, David. "A New Approach to China." Google Blog. 12 January 2010. (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html). 14 February 2010.
[59] *Ibid.*
[60] Zetter, Kim. "Google Hackers Targeted Source Code of More Than 30 Companies." Threat Level. Wired. 13 January 2010. (http://www.wired.com/threatlevel/2010/01/google-hack-attack/). 15 February 2010
[61] Drummond, David. "A New Approach to China." Google Blog. 12 January 2010. (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html). 14 February 2010.
[62] *Ibid.*
[63] Foster, Peter. "Chinese Hacker Training Website Shut Down." Telegraph. 8 February 2010. (http://www.telegraph.co.uk/news/worldnews/asia/china/7189287/Chinese-hacker-training-website-shut-down.html). 11 April 2010.

January by Secretary of State Hillary Rodham Clinton in a speech on internet freedom that was a sharp between-the-lines attack on China for its hard-handed grip on internet activity and repression of internet freedom.[64] Blaming hackers for actions that may have been the doing of the state itself serves dual purposes; it deflects blame from the state while giving China additional ammunition to justify its totalitarian control of the internet to help weed out hackers and make it safer for all users.

TITAN RAIN

Beginning in the early 2000s, probably Chinese actors systematically scanned, attacked, and infiltrated U.S. defense networks. Focusing mostly on the Department of Defense and its contractors, the attacks also targeted the Departments of State, Energy, and Homeland Security.[65] This series of attacks was first disclosed in mid-2005, having gone on for several years before disclosure. A parade of unnamed defense officials provided information on background regarding the case. Opinions ranged from blame of the Chinese government to others who assessed that at best hackers were using Chinese networks to disguise themselves.

Attackers gained access to unclassified systems on government networks. They pilfered sensitive but unclassified data from computers, including export-controlled technology. One analyst who followed the Titan Rain actors claimed that the attackers left behind covert beacons that allowed them to gain access to systems at a later date, permitting both further data collection as well as laying the foundations for a future malicious cyber attack.[66] According to the few who would speak in detail about the attacks, the preponderance of evidence pointed to the Chinese

[64]Clinton, Hillary Rodham. "Remarks on Internet Freedom." Department of State. 21 January 2010. (http://www.state.gov/secretary/rm/2010/01/135519.htm). 15 February 2010.
[65] Graham, Bradley. "Hackers Attack Via Chinese Web Sites; U.S. Agencies' Networks Are Among Targets." Washington Post. 25 August 2005: A01.
[66] Thornburgh, Nathan. "The Invasion of the Chinese Cyberspies." Time. 29 August 2005. http://www.time.com/time/magazine/article/0,9171,1098961-4,00.html

government, as these analysts hacked back against the attackers to map their networks and steal their tools.

Statements both on and off the record regarding Titan Rain highlight both the difficulties and the politics of attribution. One unnamed U.S. official asked: "Is this an orchestrated campaign by the PRC or just a bunch of disconnected hackers? We just can't say at this point."[67] That attacks originated from China was not sufficient to assign blame to the Chinese government; the possibility that other actors were using Chinese addresses to mask themselves prevented definitive assignment of blame. The coached language and sparse details briefed by senior government officials on background also highlights the desire to keep sensitive details of the attack a secret. In the original report in the Washington Post that announced Titan Rain to the world, the author's sources made clear that legal and policy considerations, and especially a "desire to avoid giving any advantage to the hackers", prevented them from disclosing more or making a public claim of attribution.[68]

[67] Graham, Bradley. "Hackers Attack Via Chinese Web Sites; U.S. Agencies' Networks Are Among Targets." Washington Post. 25 August 2005: A01.
[68] *Ibid.*

LESSONS FOR ATTRIBUTION

Sophisticated attackers take measures to obfuscate their activity, hopping through multiple nodes and coding stealthy programs to evade detection. Infrastructure from which attacks are launched are often stolen or hacked themselves, making the job of tying the pointy end of the cyber spear back to a specific actor often impossible. Chinese attackers nearly got away with this in the case of Aurora but used sloppy tradecraft and overreached against too many targets simultaneously. Ultimately they picked the wrong opponent in Google, which was clearly enraged and not willing to swallow its pride. Less sophisticated attackers harness criminal and malicious systems like botnets, worms, Trojans, and viruses to magnify their power and distribute attack vectors around the world. The organizers of the nebulous efforts against Estonia utilized this model, turning a symbolic protest into a cyber riot riding on the back of criminal botnets and scripted attacks for anti-Estonian hackers around the world. Defense officials will not likely see naval-inspired line-of-battle attacks with flagged government war-computers matched up against opponent war-computers in a battle of tactics and wit. Cyber attacks will emerge from the cloud.

Breaking through the cloud of obfuscation requires significant cyber-sleuthing resources, potential offensive "hack-back" operations, and most troublesome, time. Moonlight Maze highlighted how it may take years of passive monitoring of attacks to piece together enough bits of circumstantial evidence to tie attacks back to a region or country, let alone to a specific state actor or criminal element. Conducted properly and with appropriate stealth, attacks may never be properly diagnosed through passive means alone. Both Aurora and Titan Rain illustrated how, when combined with the political will to call it as they see it, victims can hack-back in self defense to crack through the layers of obfuscation protecting attackers. Google and McAfee did

not learn the technical, scary details about the Aurora attacks merely by being attacked. They struck back, spying on the enemy and tracking the data as it was exfiltrated out of their networks. But even this took time; there was almost a month-long gap between detection of the attacks and a public announcement of attribution to China. In the event that China were to attack U.S. defense systems in a far more malicious way, disabling vital systems to cause grave non-virtual harm to the U.S., waiting a month to forensically swim upstream back to the attacker systems would not be acceptable.

The case of the potential Brazilian cyber attacks on power infrastructure highlight another strain of cyber-attribution difficulties: politics. Attribution implies vulnerability. Companies and governments alike do not like to admit weaknesses, especially weaknesses that they are unable to fix in the short-term. Admitting weaknesses causes domestic political issues and especially in the realm of cyber invites malicious actors to take advantage of the announced weaknesses. If the Brazilian government or the power company were to admit that both outages were due to cyber attacks, enterprising criminal entities would begin in earnest to gain access to those systems to hold them hostage for a princely ransom. Additionally, blaming problems on physical infrastructure and taking a hit with fines may be preferable to re-engineering entire networks and the costs of increased network security.

Attribution implies a capability to detect and analyze the attacker's actions. Stealthy state-sponsored cyber attack and espionage systems are designed to go unnoticed. Announcing to the world that the victim has developed the technical capacity to detect and monitor this activity will trigger a change in operating procedure for the attacker. In some cases, the known and manageable attack is preferable to the unknown and thus unmanageable attack. This is likely the case with the Titan Rain intrusion set; its disclosure probably caused much

consternation at the Pentagon as it alerted the Chinese that their tools and tricks were being caught, triggering a change in behavior, tools, and standard operating procedures.

Publicly declaring the identity of the assessed perpetrator of cyber attacks can be satisfying for investigators. But once the attacks start to dissipate the fears of the unknown grow. Have the attackers learned from the disclosure how to better hide their attacks? Have they stopped? Hacking back can be stealthy as well if managed properly; public attribution of attacks may cripple these efforts to aggressively uncover enemy actions, tools, and intentions.

CONCLUSION - IMPLICATIONS FOR DETERRENCE

The set of cases analyzed here demonstrate decisively that attribution of cyber attacks is technically difficult and often politically unpalatable. Established networking protocols allow easy spoofing and obfuscation of source, destination, and intent of packets as they stream around the world. Attribution, as demonstrated in these cases, is often circumstantial at best. While victims often have strong suspicions of attackers' identities built from pieces of intelligence, the decisions of war and peace involved in a deterrence policy require a higher level of confidence than a measured hunch. To reach even elementary levels of attribution significant resources, expertise, and time are required.

The chilling suspicion of the unknown unknowns, the realization that undetected attacks may be underway at any moment, is potentially paralyzing to any deterrence policy. A deterrence policy of "I will attack you back if you attack me, but only if I find out that you did it" is not an appropriate cornerstone of a computer network defense strategy. Without a response, an attacker can assume that the victim is either unable to detect the attack or, even more emboldening, the victim is unable or unwilling to make good on its threat. Cyber attacks can be a powerful part of salami tactics on the part of the attacker. If attacks are unable to generate a deterrent response in the cyber realm, what other lines can the attacker cross?

Addressing cases where the victim state realizes that it is being attacked, Lt. Gen. Keith Alexander, director of the National Security Agency, recently proposed that his future U.S. CYBERCOMMAND would support a deterrence doctrine by attacking back in a proportional

and discriminating way against the sources of any cyber attack against the United States.[69] He extended this case specifically to those where the identities of the attackers are unknown. According to Gen. Alexander, the U.S. will attack back in accordance with the rules of engagement and in accordance with the principles of proportionality and discrimination, with the caveat that "neither proportionality nor discrimination requires that we know who is responsible before we take defensive action."[70] With statements like this, Gen. Alexander and others are providing a strong incentive for enemies of the U.S. to launch cyber attacks on the United States from third-party territory, hoping to lure the U.S. into conflict with a nation that had no role in or idea of the attack.

What the cases analyzed in this paper illustrate is that deterrence is a phenomenally poor choice as a core component in a computer network defense strategy. Bloviation and bluster, vowing deterrent responses to attacks, make for good sound bites and allow for easy porting of deep deterrence scholarship to the cyber realm. But less flashy policies and measures are more effective. Defense in depth, better security standards for software and hardware, robust computer network intelligence systems, and information sharing between and among industry and government are all good and necessary elements of a more successful computer network defense strategy. Combined with aggressive hack-back defensive measures that work to disrupt or exploit attacker infrastructure, vital networks will be better defended and deterrence as a general national policy tool will be better preserved for realms where it is more applicable.

[69] Alexander, Keith. "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command." Senate Armed Services Committee. 14 April 2010. (http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf). 15 April 2010.
[70] *Ibid*.

BIBLIOGRAPHY

Adams, James. "Virtual Defense." Foreign Affairs. May/June 2001.

Alexander, Keith. "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command." Senate Armed Services Committee. 14 April 2010. (http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf). 15 April 2010.

"CIA Confirms Cyber Attack Caused Multi-City Power Outage." SANS News Bites. SANS. 18 January 2008. (http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5). 15 February 2010.

Clinton, Hillary Rodham. "Remarks on Internet Freedom." Department of State. 21 January 2010. (http://www.state.gov/secretary/rm/2010/01/135519.htm). 15 February 2010.

Coalson, Robert. "Behind the Estonia Cyberattacks." Radio Free Europe / Radio Liberty. 6 March 2009. (http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html). 15 February 2010.

Drummond, David. "A New Approach to China." Google Blog. 12 January 2010. (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html). 14 February 2010.

"Estonia Blames Russia for Unrest." BBC News. 29 April 2007. (http://news.bbc.co.uk/2/hi/europe/6604647.stm). 15 February 2010.

Evron, Gadi. "Battling Botnets and Online Mobs." Georgetown Journal of International Affairs. Winter/Spring 2008:123.

Foster, Peter. "Chinese Hacker Training Website Shut Down." Telegraph. 8 February 2010. (http://www.telegraph.co.uk/news/worldnews/asia/china/7189287/Chinese-hacker-training-website-shut-down.html). 11 April 2010.

Graham, Bradley. "Hackers Attack Via Chinese Web Sites; U.S. Agencies' Networks Are Among Targets." Washington Post. 25 August 2005: A01.

Halpin, Tony. "Estonia Accuses Russia of 'Waging Cyber War.'" Times Online, 17 May 2009. (http://www.timesonline.co.uk/tol/news/world/europe/article1802959.ece). 15 February 2010.

James Hendler, as cited in Waterman, Shaun. "Analysis: Who Cyber Smacked Estonia?" United Press International. 11 June 2007. (http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/). 15 February 2010.

Hypponen, Mikko. "9th of May." F-Secure Weblog. F-Secure. 9 May 2007. (http://www.f-secure.com/weblog/archives/archive-052007.html). 15 February 2010.

"Information Security: Challenges to Improving DOD's Incident Response Capabilities." U.S. General Accounting Office. March 2001. (http://www.gao.gov/new.items/d01341.pdf). 15 February 2010.

Kurtz, George. "Operation 'Aurora' Hit Google, Others." McAfee Security Insights Blog. McAfee Security. 14 January 2010. (http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/). 15 February 2010.

Loeb, Vernon. "Pentagon Computers Under Assault." Washington Post. 7 May 2001: A02.

"Major Power Failures Hit Brazil." BBC News. 11 November 2009. (http://news.bbc.co.uk/2/hi/americas/8353878.stm) 15 February 2009.

Messick, Graham. "Cyber War: Sabotaging the System." CBS News. 8 November 2009. (http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml). 15 February 2010.

Noe, Nicholas, ed., Voice of Hezbollah: the Statements of Sayyed Hassan Nasrallah. London: Verso, 2007.

Rantanen, Miska. "Virtual Harassment, but for Real." Helsingin Sanomat. 6 May 2007. (http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868). 15 February 2010.

Romero, Dennis. "L.A. Law Firm Reports Cyber Attack from China." Los Angeles Weekly. 14 January 2010. (http://blogs.laweekly.com/ladaily/city-news/law-firm-cyber-attack/). 15 February 2010.

Schelling, Thomas. Arms and Influence. New Haven: Yale University Press, 1966.

Schelling, Thomas. The Strategy of Conflict. New York: Oxford University Press, 1960.

Soares, Marcelo. "Brazilian Blackout Traced to Sooty Insulators, Not Hacker." Threat Level. Wired. 9 November 2009. (http://www.wired.com/threatlevel/2009/11/brazil_blackout/). 15 February 2010.

Thornburgh, Nathan. "The Invasion of the Chinese Cyberspies." Time. 29 August 2005. http://www.time.com/time/magazine/article/0,9171,1098961-4,00.html

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." The Guardian. 17 May 2007. (http://www.guardian.co.uk/world/2007/may/17/topstories3.russia). 15 February 2010.

Zetter, Kim. "Feds' Smart Grid Race Leaves Cybersecurity in the Dust." Threat Level. Wired. 28 October 2009. (http://www.wired.com/threatlevel/2009/10/smartgrid/). 15 February 2010.

Zetter, Kim. "Google Hack Attack Was Ultra Sophisticated, New Details Show." Threat Level. Wired. 14 January 2010. (http://www.wired.com/threatlevel/2010/01/operation-aurora/). 15 February 2010.

Zetter, Kim. "Google Hackers Targeted Source Code of More Than 30 Companies." Threat Level. Wired. 13 January 2010. (http://www.wired.com/threatlevel/2010/01/google-hack-attack/). 15 February 2010.

Zetter, Kim. "Report Details Hacks Targeting Google, Others." Threat Level. Wired. 3 February 2010. (http://www.wired.com/threatlevel/2010/02/apt-hacks/). 15 February 2010.