Know Thy Enemy: Cyber Warfare in the 21st Century
Daniel Kohlbrenner, *Entrepreneurship and Computer Science, 2017*

"It's the great irony of our Information Age - the very technologies that empower us to create and to build also empower those who would disrupt and destroy."[1] Referring to the 2010 hacking attacks on Google and several other companies in various industries, President Obama demonstrates the new type of threat that the world is facing: Cyber Warfare. Dozens of major hacks have occurred this past August alone - from the theft of UPS consumer information, to the politically-motivated attacks on Delaware's treasury division by the anti-Israel group SaLeM.[2] "We have never ever, outside of the defense industry, seen commercial industrial companies come under [this] level of sophisticated attack," said Dmitri Alperovitch, vice president of threat research at McAfee, Inc., a cyber security firm.[3] It is clear that the frequency of these attacks are increasing, as is the need for a proper defense against them. Yet while something must be done, current U.S. strategies, specifically those of the intelligence industry over the past decade, have been undermining U.S. national defense goals.

Although "Cyber Warfare" has many meanings in the media, it is most commonly defined as a technology-based conflict involving the use of information systems.[4] While previous wars have been fought on the ground, in the water, and up in the air, the next realm of battle will be cyberspace. This new form of warfare utilizes the complexities of digital society for the sake of military, political, and economic gains.

The use of Cyber Warfare predates the Internet. Following World War I, a German engineer named Arthur Scherbius invented a new and powerful way to code military messages called "Enigma." The subsequent development of the machine "Ultra" led to the Allies' massive advantage over the Germans in later years. Although post-WWI encryption machines seem like ancient history, it demonstrates the type of arms race that continues to this day. Post-9/11 doctrine demanded that the government have the capability to identify potential threats and to stop future plots before they unfold, leading to a massive increase in cyber operations by Western intelligence agencies. But like the advancement in every other type of warfare, there is potential for unintended consequences.

In recent years, governments around the world have upgraded their intelligence capabilities creating what some refer to as "cyber armies."[5] The justification for expansion has been to track terrorist communications. In effect, there has been a massive increase in state-sponsored programs to identify and track potential enemies. These intelligence agencies work with allies around the world to conduct surveillance and perform cyber-attacks against *both* foreign and domestic threats.

The existence of domestic targets highlights an important aspect of cyber warfare: there are no real geographic boundaries. While government collectives have huge amounts of resources, small groups of hackers operating anywhere in the world can pose a very serious threat. Anonymous, a techno-political hacker movement, was credited with attacks on key systems of the Egyptian government during the Arab Spring.[6] Western powers have thus realized the

threat of small asymmetric groups and in turn, have created a large-scale surveillance program to analyze all digital communications for the sake of identifying these threats.

One of the more controversial methods of this strategy is the collection of metadata. Metadata is information about specific communications such as phone and internet conversations. While it doesn't collect the content of conversations, it does include data such as who the individuals are, how long they speak, and where each individual is physically located.[7] Malte Spitz, a German politician, successfully sued the telecom companies for access to his metadata. What was returned was information regarding everywhere that he had been and everyone he communicated with over six months. While a single instance of this data may not be alarming, when stitched together, it forms an alarmingly detailed map of an individual's life.[8] This practice is controversial because it can be easily used by individuals and governments with malicious intent. Already, it's clear the collection of metadata can be abused in many ways; from spying on individuals with no suspicion of criminal activity to identifying those who are likely to dissent against the ruling government.[9][10] Indiscriminate surveillance has proven to be ineffective at stopping terrorists, while completely undermining the citizen's right to privacy. In fact, an in-depth analysis of the 225 terrorism cases since 9/11 showed that the collection of metadata has "no discernible impact on preventing acts of terrorism."[11] While demeaning the citizen's right to privacy, these programs provide shockingly little security from the threats that supposedly justify their existence.

As much of this metadata is forcibly taken from U.S.-based technology companies, the U.S. intelligence apparatus also has had a discernible economic impact. When Yahoo first resisted U.S requests for access to user data, Yahoo was threatened with fines upwards of $250,000 for every day that it refused to comply.[12] Since then, U.S. companies that store valuable user data have been forced into handing over information about their clients. Companies who comply with government data requests are issued gag orders, so they remain quiet on the number of requests they receive. These practices are all done under the pretense of national security, without any tangible evidence of the efficacy of such data collection.

In response to the state's use of the Patriot Act, there has been an exodus of tech companies moving their data outside of the United States out of fear of draconian legislation.[13] As the U.S. intelligence community continues to strong-arm tech companies, many global leaders chose not to store their data in the U.S. and instead seek privacy havens such as Germany for shelter. This degrades international trust in the technology sector, throttling innovation and preventing multi-million dollar contracts with U.S. firms out of fear of snooping.[14]

Is this data strategy worth the damage that it incurs? Human rights advocates consider the coercion of the U.S. tech-industry a disturbing trend, but several leading security experts also suggest that U.S. surveillance tactics actually weaken cyber-infrastructure, leaving us vulnerable to future attacks. Famously, Edward Snowden's leaks revealed that intelligence agencies have been forcing tech companies to install secret back doors into all of their commonly used products. At the same time, they worked to weaken encryption, the type of security meant to conceal communications. Researchers from the U.K. later published a report claiming that the activities of the NSA and the U.K.'s Government Communications Headquarters (GCHQ) have

weakened the global cyber framework overall.[15] While these back doors make it easier to conduct surveillance, independent criminals can use these security holes for their own ends.[16] Bruce Schneier, a fellow at Harvard's Berkman Center for Internet and Society, accuses the NSA stating: "By deliberately undermining online security in a short-sighted effort to eavesdrop, the NSA is undermining the very fabric of the internet."[17] While Western intelligence agencies create holes in collective security, the threat of state-sponsored cyber attacks is on the rise.

One of the most potent depictions of Cyber Warfare occurred in 2009, when executive officials revealed that there had been a joint operation between the NSA and Israel's cyber division,Unit 8200,c ode-named "Olympic Games." The operation began in 2006 as a program to develop cyber weapons to be used against Iran.[18] Since then, these operations developed weapons like STUXNET, Flame, and Duqu. These weapons were used to create blueprints of Iranian nuclear facilities, and later used to cripple those facilities by increasing the pressure on spinning centrifuges. The viruses spread to several sites across Iran through the use of infected thumb-drives. This activity exhibits the ease at which cyber operations can be deployed. With critical infrastructure open to thousands of employees and contractors, a team of foreign operatives do not need guns to cripple a country's infrastructure. All they need is a well-coded virus and a thumb-drive. Once the malicious drive is plugged into a company computer, a program will execute tasks ranging from destruction of files, to stealing valuable company data. As one of STUXNET's architects said, "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."[19] These attacks occurred during nuclear talks with Iran, and when it was discovered, what little trust did exist between the two nations was severely damaged.

The NSA has also been operating in close relationship with U.S. drone operations in Yemen and Somalia. Journalists Jeremy Scahill and Glenn Greenwald revealed that the NSA identifies and tracks targets whose metadata fit a certain profile. The NSA then adds whoever is in possession of the phone that fits this pattern of behavior to a kill-list.[20] As a former Joint Special Operations Command and drone operator stated: "We're not going after people; we're going after phones in the hopes that the person on the other end of that missile is a bad guy."[21] Not only has this procedure led to several unidentified innocent persons being targeted and killed, but it also demonstrates the close relationship that U.S. "Cyber War," in the form of surveillance, has with actual military and civilian deaths.

Weaponized cyber attacks seem to be the winning strategy for this new kind of warfare. Such attacks provide an easier and more cost-effective way to cripple foreign infrastructure. without having to declare war or take the same level of accountability that other military operations would necessitate. Logic would dictate that if so much emphasis was put on offensive cyber operations, the U.S. must be equally prepared to defend domestic critical institutions from foreign adversaries. Unfortunately, this isn't the case. Other governments use similar cyber techniques to harm U.S. national security. Earlier this year, the U.S. filed criminal charges against five Chinese military officials, accusing them of militarized attacks on six key American energy and metal companies. Attorney General Eric Holder went on to state that the U.S "will not tolerate foreign government efforts to sabotage American companies."[22] Although popular rhetoric states that the U.S. takes these threats seriously, the priority of U.S. intelligence

apparatus is to take an offensive approach, rooting out potential threats at the detriment of U.S. domestic security.

Human rights and constitutional concerns aside, current U.S. policy involving Cyber Warfare is miscalculated. While U.S. intelligence agencies focus on preemptively spying and attacking potential enemies, they create serious vulnerabilities in critical infrastructure exposing American citizens to retaliation from U.S. enemies. As a result, technology companies are pressured to relocate and hide their data outside of the U.S. Intelligence agencies seem follow the philosophy "to find the needle, collect the entire haystack." This philosophy has weakened the U.S. both economically and technologically all while eroding civil liberties and doing very little to prevent terrorist attacks.

So what can be done? Given the ease that these systems can be deployed and the power that they give the state, it is unlikely that governments will end these practices anytime soon. The cyber arms-race continues to this day, and as long as its policies are considered classified, any serious debate on their safety is futile.

Until international standards can be created to address this new form of warfare, the best deterrence is a population who is energetic against this threat. Organizations need to be more proactive about fixing security holes. For users, it is paramount to encrypt computer and internet traffic.[23][24] Technological understanding is the literacy of the 21st century. Whether its governments, hackers, or automated viruses, the Internet is filled with predators trying to grab valuable personal data. Whenever you log online, you're entering the jungle. As more and more personal information is digitized, it becomes a matter of self-defense to guard against this new threat of cyber warfare.

[1] Remarks by the President on Securing Our Nation's Cyber Infrastructure (The White House)
http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

[2] Hackmageddon.com (Hackmageddoncom)
http://hackmageddon.com/category/security/cyber-attacks-timeline/

[3] Google Hack Attack Was Ultra Sophisticated, New Details Show | WIRED (Wired.com)
http://www.wired.com/2010/01/operation-aurora/

[4] cyberwarfare (What is ?)
http://searchsecurity.techtarget.com/definition/cyberwarfare

[5] New cyber reserve unit created (- News stories)
https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit

[6] Anonymous and the Arab uprisings (Al Jazeera English)
http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html

[7] metadata (What is ?)
http://whatis.techtarget.com/definition/metadata

[8] http://opendata.zeit.de/widgets/dataretention/ (ZEIT ONLINE)
http://www.zeit.de/datenschutz/malte-spitz-data-retentio

[9] Edward Snowden Testimony @ Parliamentary Assembly of the Council of Europe (PACE) - 04/08/2014
http://www.youtube.com/watch?v=3f8Lunf1a2w

[10] How Paul Revere could have been outed as a ‘terrorist’ by metadata (Washington Post)
http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/17/how-paul-revere-could-have-been-outed-as-a-terrorist-by-metadata/

[11] NSA phone record collection does little to prevent terrorist attacks, group says (Washington Post)
http://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html

[12] Rushe, Dominic. "Yahoo $250,000 Daily Fine over NSA Data Refusal Was Set to Double 'every Week'" The Gaurdian. September 12, 2014. Accessed September 14, 2014.
http://www.theguardian.com/world/2014/sep/11/yahoo-nsa-lawsuit-documents-fine-user-data-refusal.

[13] Foreign Businesses Flee US Cloud Computing, Survey Finds - InformationWeek (InformationWeek)
http://www.informationweek.com/cloud/software-as-a-service/foreign-businesses-flee-us-cloud-computing-survey-finds/d/d-id/1113385

[14] Facebook, Google and Apple lobby for curb to NSA surveillance, Samuel Gibbs - (The Guardian)
http://www.theguardian.com/technology/2014/nov/17/facebook-google-apple-lobby-senate-nsa-surveillance

[15] How NSA weakens encryption to access internet traffic (- tech)
http://www.newscientist.com/article/dn24165-how-nsa-weakens-encryption-to-access-internet-traffic.html#.VCRcjvldX1Y

[16] Bristol Cryptography Blog (: Open Letter From UK Security Researchers)
http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html

[17] Greenwald, Glenn, James Ball, and Julian Borger. "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security." The Gaurdian. September 5, 2013. Accessed September 7, 2014. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[18] Obama Administration Admits Cyberattacks Against Iran Are Part Of Joint US-Israeli Offensive (Business Insider)
By: Kelley, Michael.
http://www.businessinsider.com/obama-cyberattacks-us-israeli-against-iran-2012-6#ixzz1wYnaa3jK

[19] The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought (Business Insider)
By: Kelley, Michael.
http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

[20] Death By Metadata: Jeremy Scahill & Glenn Greenwald Reveal NSA Role in Assassinations Overseas (Democracy Now!)
http://www.democracynow.org/2014/2/10/death_by_metadata_jeremy_scahill_glenn

[21] Jeremy Scahill: NSA Using Cell Phone Metadata For Obama's Kill List (YouTube)
http://www.youtube.com/watch?v=6_ojdb_WqdU

[22] US declares cyber war on China: Chinese military hackers charged with trying to steal secrets from companies including nuclear energy firm (The Independent)
http://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-metals-and-solar-product-industries-9397661.html

[23] How to encrypt (almost) anything (PCWorld)
http://www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html

[24] Learn to Encrypt Your Internet Communications | EFF Surveillance Self-Defense Project (Learn to Encrypt Your Internet Communications | EFF Surveillance Self-Defense Project)
https://ssd.eff.org/wire/protect/encrypt

Consulted Works

The Snowden Effect: Yahoo To Join Gmail In Offering Users End-To-End Encryption (Forbes)
http://www.forbes.com/sites/kashmirhill/2014/08/07/yahoo-end-to-end-encryption/

Defcon 21 - Unexpected Stories - From a Hacker Who Made It Inside the Government (YouTube)
http://www.youtube.com/watch?v=h9wXq6oRBnI

Thanks, NSA: 25% of UK and Canadian businesses are moving data outside the US, says report (PandoDaily Thanks NSA 25 of UK and Canadian businesses are moving data outside the US says report Comments)
http://pando.com/2014/01/08/thanks-nsa-25-of-uk-and-canadian-businesses-are-moving-data-outside-the-us-says-report/

The Cyber War Threat Has Been Grossly Exaggerated (– IQ2 Debates)
http://intelligencesquaredus.org/debates/past-debates/item/576-the-cyber-war-threat-has-been-grossly-exaggerated

NSA Fears Prompt Companies to Move Data Out of U.S. (The CIO Report RSS)
http://blogs.wsj.com/cio/2014/01/08/nsa-fears-prompt-companies-to-move-data-out-of-u-s/

ACLU v. NSA: The Challenge to Illegal Spying (American Civil Liberties Union)
https://www.aclu.org/national-security/aclu-v-nsa-challenge-illegal-spying

How Cybersecurity Has Changed Since 9/11 (PCMAG)
http://www.pcmag.com/article2/0,2817,2392642,00.asp