Maj Terrance S. Allen
CGSC US Air Force Element

A Clear Deterrence Strategy Required for Cyber Going Forward

Introduction

With the press of a button, war is launched against a nation. Much of the nation's civilian's livelihood will be destroyed with this button press. Within the US, there is an operator ready to hit their button, ensuring a devastating retaliatory attack. This scene played out during the cold war, with the US and Soviet Union both ready to ensure destruction of the other, should a nuclear launch ensue. Thankfully, the world did not live through the aftermath if these buttons were pressed. Today, we live through a scenario very much like this, but with different weapons and actors. Instead of only a few countries with the capability to conduct nuclear warfare, cyberwarfare can be conducted by anyone with a computer and basic hacking skills. Just like nuclear war changed the conduct and threatened total war, cyber has the potential to do the same. The growing appetite for cyber by militaries and civilians led to a very "connected" world where an attack has the potential to spread outside military targets. There is no clear definition of what is considered cybercrime or cyberwar. One countries interpretation may simply be based on what side of the attack they are on. The US needs to take the lead and codify what is cybercrime, what is cyberwar, and develop a clear strategy on how best to deter future attacks on American targets.

A Change in Warfare: Nuclear Weapons

After the US dropped the atomic bombs on Japan in WWII, it woke the world to the real and devastating potential of nuclear weapons. Other countries were conducting nuclear research before the US, but this public employment of weapons changed what warfare was capable of in a single shot. With two bombs, Nagasaki endured 75,000 killed or wounded with 1/3 of the city devastated[1], while Hiroshima suffered “130,000 killed, injured or missing, and 90% of the city was leveled.”[2] Countries worked in the period after the war to gain their own nuclear weapons to have power themselves. By the middle of the 20th century, many military experts and political leaders feared a proliferation of nuclear weapons throughout the world, with many countries crossing the threshold from nuclear research for peaceful purposes into military uses.[3] This race could cause many countries to cross the nuclear threshold and bring the world to an arms race. In the 1960s, 21 South American countries had already agreed to limit the pursuit of nuclear military weapons through the Treaty of Tlatelolco.[4] To limit the spread of weapons throughout the world, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) was created and opened for signature on 1 July, 1968. At the time of the treaty, only five countries possessed nuclear weapons: the United States, Soviet Union, United Kingdom, France, and China. It was clear many at the time, that without a good framework to limit the pursuit of nuclear weapons, many other countries would cross the nuclear military threshold, a serious danger to the civilizations of the world. This treaty continues through today with most countries adhering to the rules established by it.

A Change in Warfare: Take 2

The destructive nature of nuclear weapons dramatically changed the effects of warfare. This is not new in the history of war. The inventions of the longbow, gunpowder, machine gun, aircraft, tanks, and nuclear weapons all shifted the nature of war and forced a paradigm change if nations wanted to remain relevant. Cyber also changed the nature of war, but the question is: do countries currently view cyber as a new phenomenon, or do they recognize it is already here? The SANS Institute points out, "in this digital age warfare is no longer limited to military versus military engagements. In the cyber-world, a digital enemy can bypass our military and take down what is near and dear to us. Destroying critical national infrastructure such as automated power plants, stock markets, and transportation systems could disable this nation without firing a shot."[5] This shift in capabilities will be debated among military theorists if it was/is a military revolution, or a revolution in military affairs. At this point, it does not matter. Recognition it already began and will become part of conducting future war is critical. Nations who fall behind developing cyber capabilities will find themselves strategically behind just like when nuclear weapons were used by the US and when Desert Storm occurred. Future developments will likely shift how current military strategists envision future use of cyber, but it will be used.

Growing Appetite for Cyber

An article published by the SANS Institute in 2004 noted that due to the great advances in information and communications technology, there is an unprecedented impact of cyber on our society. Much of our life is dependent upon the cyberspace realm. National infrastructure, transportation systems, government sectors, and many other private and public companies rely heavily on computers and networks systems.[6] 13 years after this article was published, nations are even more dependent on technology for everyday life. The appetite for technology is not slowing down, but growing faster. More devices are “connected” and while life may seem easier for some, the effects of a cyber-attack are more wide ranging. An attack on one of part of the system could have a significant impact on the daily lives of many. One example could be the targeting of a utility business. The attacker targets the power plant and shuts down integral components. If this plant is the only power source for an area, then this area is without power. While not immediately life critical, should this situation continue with no power coming in, the effects begin to grow. It is feasible the cause of the shutdown would be discovered and the plant brought back up. But for how long, and did the attack do any permanent damage? Though this situation is a temporary effect, concern must still be given to the connectedness of today's world.

Cheap Form of Attack

Though cyber warfare could disrupt a large portion of a community with just one push of a button, it is different from nuclear weapons because unlike the technological requirements to employ nuclear weapons, anyone with access to a computer and hacking tools can become a cyber actor. If one does not possess the knowledge to conduct sophisticated cyber-attacks, they could look for disgruntled programmers who want sell their abilities to another buyer[7] and give them an upper hand on the code they developed. Due to the cheap nature of conducting an attack, this is an effective way for various groups with different motivations and other non-state actors to wage war against a technologically dependent/superior nation. This includes criminals looking for money, cyber terrorists who are fighting on behalf of religious or cultural ideals, corporate espionage, inside employees who are looking to embarrass the company, and even just simple hackers who are looking to test out new tools for hacking other entities.[8] The difference between all these groups are the motivations behind conduction cyber-attacks.

Proportionality, Indiscriminate Attacks, and Unintended Consequences.

When nuclear weapons were first developed, they were not on precision guided munitions. Today, the technology exists for kinetic weapons to accurately hit targets and reasonably limit collateral damage. Cyber though, cannot be used like a precision guided munition. You cannot always quickly identify the effects the weapon had and see the collateral damage. As noted by Davis, "cyber war is not in the same league as a nuclear war or even kinetic war with precision weapons in so far as "assuring" anything, much less long-term incapacitation or distraction. Collateral effects and related confusion are likely."[9] This leads to a problem of determining if the attack through cyber would blur the lines of an indiscriminate attack, or “distinguishing between the civilian population and combatants and between civilian objects and military objectives.”[10] If a country were to retaliate through offensive cyber weapons, proportionality must be considered. Proportionality looks at legally deciding if “attacks are prohibited if they cause incidental loss of civilian life, injury to civilians, or damage to civilian objects that is excessive in relation to the anticipated concrete and direct military advantage of the attack.”[11] Cyber has unintended consequences when used in an offensive capacity. Like nuclear weapons, potential effects of cyber weapons are not guaranteed to be limited to just military targets when used. For example, if a virus were used against a network, it is plausible the virus could be coded to attack specific items. However, the virus could spread further than thought. If the US limits military action to combatants, then is using a cyber weapon which unintentionally affected civilians considered the same as a kinetic weapon which misses the intended target, or causes collateral damage? Does this lead the US to be guilty of indiscriminate attacks? Due to the connected nature of many nations and individuals now, it is difficult to conduct a large cyber-attack without affecting civilians. The original target maybe hit, but the second and third order effects may spread out further than intended, as it is difficult to sift through the millions of lines of code devices use today. The F-35 itself contains over “8 million lines of software code – more than four times the amount of the world’s first 5th generation fighter, the F-22 Raptor.”[12]

Many other devices contain as much or more code, with some companies reaching into the billions.[13] Though the simplicity of the code changes between platforms, the simple fact there are so many lines of code makes it difficult to accurately know exactly what some actions may cause.

Cybercrime vs. Cyberwar

Two recent examples demonstrate the difficulty in distinguishing between cybercrime and cyberwar. In 2013, the Associated Press (AP) Twitter account was hacked. A false story was posted which claimed there were two explosions at the White House and President Obama was injured. This sent stock markets spiraling and $136 Million dollars was lost. The AP quickly got control back of their twitter account, but the damage was done. Eventually, the stock market made the money back.[14] Does this count as cybercrime? Was it cyberwar? The hack was eventually traced back to the "Syrian Electronic Army, which backs but is not officially sponsored by the Syrian government."[15] Real damage was done, so does this rise to the level of cyberwar and warrant a military response? A second example is the Russian cyberwar against Ukraine. Attacks on Ukrainian networks targeted classified intelligence to include the number of troops in reconnaissance battalions and types of equipment used. After this attack was found and Ukraine publicly declared it was the Russian security service, the same organization changed their code and got back into the systems. After a cease-fire was negotiated, the attacks stopped.[16] Does this mean the organization within Russia considered their actions attacks, since they stopped after the cease-fire? Also, if the cease-fire saw a stop to the actions, certainly there was control by Russia over the groups, enough that if they were not government sanctioned, the government got them to stop at the same time as the cease-fire. This would seem to implicate the Russian government with at least sponsoring the attacks. But does this take it from a cybercrime to cyberwar? The second example closely aligns with espionage, but was conducted in concert with kinetic military actions. Yet no international military action was taken on either example. This causes problems for classifying future cyber-attacks without clearly articulating the lines between what is cybercrime and cyberwar.

Deterrence

Paul K. Davis wrote "deterrence by itself is a fragile basis for strategic thinking."[17] He also stated that "hoping for a deterrent with today's reality would be like grasping for straws. Deterrent measures should definitely be part of a larger strategy, but the focus should be elsewhere."[18] Because cyber war is cheap to fund and there are many different motivated groups out there, deterrence similar to MAD is not a viable option, as it was for nuclear weapons. Unlike nuclear weapons, the offensive capability of cyberspace is not limited to nation states. Any individual can go down to a store and buy a computer, look on the Internet for basic hacking tools, and then begin practicing from any computer connected to the internet. Cyber deterrence would not be just against another nation, but an entire spectrum to include criminal organizations, hackers, and state-sponsored groups. This is a large reason why a singular deterrent policy would suffer across the cyber spectrum. Technology exists to spoof your actual location and make it seem you are somewhere else. This creates problems when trying to attribute blame for the attack.[19] If you can’t figure out who did it and why, you struggle to fight against it. The war becomes unclear. By the time countries figure out where it came from, the damage may already be done and any action taken will be too late. A future deterrence policy must be flexible enough to deal with all the actors and the varied motivations spurring them on.

Conclusion

If anyone is unsure if cyberwar is here, it is. It was not introduced to the world like the nuclear bomb, but was gradually tested and its usage increased by organizations seeking to gain an advantage over their adversary. Though the destructive power (temporary in nature) is similar to nuclear weapons with respect to a large area affected instantaneously, a deterrence strategy like MAD would not work due to the wide range of entities capable of conducting cyber-attacks. The deterrence strategy needs to be flexible enough to detract criminal organizations through judicial punishments, as well as state actors through sanctions ranging from economic up to and including military action. There needs to be an articulated response if the US were to be attacked by a nation state. Something similar to an escalation ladder concept used after World War II. This prevents an either/or situation, or redline proclamation, where if you don't act, your credibility is shot. Having a wide range of options would allow for a measured response to demonstrate the resolve to protect national interests based on who the threat was coming from. A future treaty for cyberwar should use some principles of the proposal put forth by Richard A. Clark and Robert Knake, and include imposing a ban on first use cyber-attacks against civilian infrastructure. This ban could be in place only during times of peacetime operations. If two nations were to go to war, either a cyber war where one nation was attacked first, or a shooting war, this ban would then be lifted.[20] The merits of this proposal lay a foundation for nations to have a common agreement pertaining to what is acceptable with the use of cyber-attacks against another nation. The international community needs to come together and define what constitutes cybercrime and cyberwar, as the lines between the two are blurred at best. The definition should start with the motivation of the group conducting the attack and the intended purpose of the attack. Then build out from there. These definitions are needed to allow countries to seek appropriate justice within the international community. These actions will allow the US to more effectively deter cyber-attacks and get ahead of nations who already employ cyber without regard to international norms, as there are no clear rules agreed to by all parties.

[1] *The Columbia Encyclopedia*, 6th ed., s.v. "Nagasaki," http://www.encyclopedia.com/places/asia/japanese-political-geography/hiroshima#1E1Hiroshim (accessed 26 March 2017).

[2] *The Columbia Encyclopedia*, 6th ed., s.v. "Hiroshima," http://www.encyclopedia.com/places/asia/japanese-political-geography/hiroshima#1E1Hiroshim (accessed 26 March 2017).

[3] Nobel Media, "The Development and Proliferation of Nuclear Weapons," *Nobelprize.org* (2014). http://www.nobelprize.org/educational/peace/nuclear_weapons/readmore.html (Accessed 26 March 2017).

[4] Nobel Media, "The Development and Proliferation of Nuclear Weapons."

[5] SANS Institute, "Information Warfare: Cyber Warfare Is the Future Warfare," *Global Information Assurance Certification Practical Repository* (2004). https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165 (accessed 26 March 2017).

[6] SANS Institute, "Information Warfare: Cyber Warfare Is the Future Warfare."

[7] SANS Institute, "Information Warfare: Cyber Warfare Is the Future Warfare."

[8] SANS Institute, "Information Warfare: Cyber Warfare Is the Future Warfare."

[9] Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf (accessed 26 March 2017).

[10] Roy Gutman and Daoud Kuttab, "Indiscriminate Attack," Crimes Of War, 2011, http://www.crimesofwar.org/a-z-guide/indiscriminate-attacks/ (accessed 26 March 2017).

[11] Horst Fischer, "Proportionality, Principle Of," Crimes of War, 2011, http://www.crimesofwar.org/a-z-guide/proportionality-principle-of/ (accessed 26 March 2017).

[12] "A Digital Jet for the Modern Battlespace," Lockheed Martin, https://www.f35.com/about/life-cycle/software (accessed 26 March 2017).

[13] Cade Metz, "Google Is 2 Billion Lines of Code-And It's All in One Place," Wired, September 16, 2015, https://www.wired.com/2015/09/google-2-billion-lines-codeand-one-place/ (accessed 26 March 2017).

[14] Max Fisher, "Syrian Hackers Claim Ap Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?," The Washington Post, April 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.7d6e08abb0aa (accessed 26 March 2017).

[15] Fisher, "Syrian Hackers Claim Ap Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?"

[16] Aarti Shahani, "Report: To Aid Combat, Russia Wages Cyberwar Against Ukraine," NPR, April 28, 2015, http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine (accessed 26 March 2017).

[17] Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf (accessed 26 March 2017).

[18] Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar."

[19] Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar."

[20] Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar."