A Clear Deterrence Strategy Required for Cyber

by Terrence S. Allen

With the press of a button, a nation goes to war. Much of that nation's livelihood will be destroyed with this button press. In the U.S. there is always an operator ready to hit their button, ensuring a devastating retaliatory attack. This was the scene during the Cold War, with the U.S. and Soviet Union both ready to ensure destruction of the other, should a nuclear launch ensue. Thankfully, that situation never occurred.

Today we live in a scenario very much like this, but with different weapons and participants. Instead of only a few countries with the capability to conduct nuclear warfare, strategic offensive cyberspace operations (OCO) can be conducted by anyone with a computer and network access. Just as the threat of nuclear war changed the conduct of warfare and threatened total war, strategic cyber weapons have the potential to do the same. Unfortunately there are no clear definitions for what is considered cyberwar versus cybercrime. A country's interpretation between the two might simply be based on what side of the attack they are on. The U.S. must take the lead by defining what cyberwar is, what cybercrime is, and formulate a clear strategy on how best to deter future attacks on American targets.

A Change in Warfare: Nuclear Weapons

After the U.S. used atomic bombs on Japan in WWII, it awoke the world to the real and devastating potential of nuclear weapons, changing the paradigm of warfare. This type of technological driven change is not new in the history of war. Technological advances such as the inventions of the longbow, gunpowder, machine guns, aircraft, and tanks all shifted the nature of war and forced paradigm changes. With two bombs, Nagasaki suffered 75,000 killed or wounded and 1/3 of the city devastated[1], while Hiroshima had 130,000 killed, injured or missing and 90% of the city was leveled.[2] Countries in the post-war period worked to obtain their own nuclear weapons. By the middle of the 20th century, many military experts and political leaders feared a proliferation

Major Terrence S. Allen is an Airborne Warning And Control System pilot currently assigned to School of Advanced Air and Space Studies at Maxwell Air Force Base. He earned his Masters in Military Operational Art and Science, and deployed multiple times in the U.S. Central Command area of operations.

of nuclear weapons throughout the world, with many countries crossing the threshold from nuclear research for peaceful purposes into military uses.[3] By the 1960s, twenty-one countries had already agreed to limit their pursuit of nuclear military weapons through the Treaty of Tlatelolco.[4] And to limit the spread of nuclear weapons throughout the world, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) was initiated. 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 to 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 civilized world. The NPT continues through today with most countries adhering to the rules. A similar framework to what gained international agreement on the use and proliferation of nuclear weapons could work for an agreement on strategic OCO. Further, it is very much needed as soon as possible before individual nation states develop their own definitions and normalize OCO weapon use, allowing by default the cyber domain to become similar to the wild west of the U.S. during the 1800s.

A Change in Warfare: Strategic Offensive Cyberspace Operations

Cyber, like nuclear weapons, has changed the nature of war; but, the question is do individual countries as well as the international community view cyber as an emerging phenomenon, or do they recognize it is already here? The SysAdmin, Audit, Network and Security (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] OCO has forced a new paradigm of warfare. Nations failing to develop cyber capabilities will find themselves strategically behind other countries. Future developments will shift how current military strategists envision the future use of cyber, and make no mistake, it will be used. Nations must invest the time and resources to develop thoughts on those future uses so as to create defensive strategic cyber weapons and strategies to deter attacks. The growing interconnectedness of civilian and military use of cyberspace makes this essential.

[Offensive Cyberspace Operations - OCO] has forced a new paradigm of warfare.

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 civilian and military 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] Thirteen years after this article was published, nations are even more dependent on technology for everyday life. The necessity for technology is not slowing down, but growing faster. Now, with more devices being "connected" that make life easier for so many, the effects of a cyber-attack are more wide ranging. An attack on one part of the system would have a significant impact on the daily lives of many. For one example look at the targeting of a utility business. An 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. If this situation continues, the effects begin to grow from inconvenience and loss of

monetary transactions, to potential loss of life if the attack is not repealed. A clear and coherent strategy communicated to adversaries, both nation-states and criminal organizations, is vital to dissuading attacks where the second and third order effects are against non-combatants. This messaging is critical to a complete deterrence strategy implemented by nation states.

...discovering the true motivations ...and understanding if the attacks are state sponsored...are key to determining the appropriate response by the attacked nation.

Cheap Form of Attack

Though cyber warfare could disrupt a large portion of a community with the push of a button, it is different from nuclear weapons. Unlike the technological requirements to employ nuclear weapons, anyone with access to a computer and hacking tools can become a cyber attacker. If one does not possess the knowledge to conduct sophisticated cyber-attacks, they could look for disgruntled programmers who want to sell their abilities to another buyer.[7] Due to the relatively cheap nature of conducting an attack, this is an affordable way for various groups with different motivations and other non-state actors to wage "war" against a technologically dependent nation. This includes criminals seeking money, cyber terrorists who are fighting on behalf of religious or cultural ideals, corporate espionage, employees who are looking to embarrass their company, and hackers who are looking to simply test out new tools for hacking other entities.[8] While the results of cyberattacks are often similar, the motivations of the various attackers may vary greatly. Thus discovering the true motivations behind the attackers and understanding if the attacks are state sponsored, or even state conducted, are key to determining the appropriate response by the attacked nation.

Cybercrime vs. Cyberwar

Two examples demonstrate the difficulty in distinguishing between cybercrime and cyberwar. And the ease of the attacks increase the chance future attacks will be mischaracterized as enemy OCO, leading to unintended escalations. In 2013, the Associated Press (AP) Twitter account was hacked. A false narrative appeared which claimed there were two explosions at the White House and President Obama was injured. This sent stock markets spiraling and $136 million dollars were temporarily lost. The AP got control back of their twitter account within 30 minutes, but the damage was done. Eventually, the stock market made the money back.[9] Was this hack attack a cybercrime or 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."[10] Real damage was done, though temporarily, so did this rise to the level of a state sponsored cyberwar and thus warrant a military response?

The second example closely aligns with espionage, but was conducted in concert with kinetic military actions - 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 the initial cyberattack, the same organization changed their code and got back into the Ukrainian systems. After a cease-fire of kinetic military operations was negotiated the cyberattacks stopped.[11] Does this mean the cyber organization within Russia considered their actions attacks, since they stopped after the government agreed cease-fire was negotiated? Also, since the cease-fire saw a stop to the cyberattacks, this seems to indicate there was control by Russia over the cyberattack

groups, enough so that even if they were not government sanctioned, the government got them to stop at the same time as the cease-fire. Was this a cybercrime stealing information or was this cyberwar? These examples illustrate the difficulty in classifying future cyberattacks because there is no clearly articulated, commonly accepted, and internationally agreed to, definitions as to what defines a cybercrime versus cyberwar.

Proportionality, Indiscriminate Attacks, and Unintended Consequences

When nuclear weapons were first developed, they were not precision guided munitions. Today, the technology exists for kinetic weapons to accurately hit targets and reasonably limit collateral damage. However, cyber cannot be used like a precision guided munition. One cannot always correctly identify the effects of the weapon 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."[12] This leads to a problem of determining if the cyber-attack crosses the line of an indiscriminate attack. For example, if a virus were used against a network, the virus would be coded to attack specific items. However, the virus could spread further than desired. The U.S. and other nations attempt to limit conventional military effects to combatants. When a weapon misses the target, the international community gets involved with discussions on the reasons non-combatants were affected. Is using a cyber weapon which unintentionally affects civilians considered the same as a kinetic weapon which misses the intended target or causes collateral damage? Does this make the US guilty of indiscriminate attacks? Due to the connected nature of many nations and individuals, it is difficult to conduct a large cyber-attack without affecting non-combatant civilians. The original target maybe hit but the second and third order effects may spread out further than intended. If a country retaliates via OCO 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."[13] Cyber has unintended consequences when used in an offensive capacity. Like nuclear weapons, potential effects of strategic OCO weapons are not guaranteed to be limited to just military targets.

Cyber has unintended consequences when used in an offensive capacity.

Deterrence

Paul K. Davis wrote "deterrence by itself is a fragile basis for strategic thinking."[14] 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."[15] Because cyber war is cheap to fund and can be conducted by many differently motivated groups, deterrence similar to MAD is not a viable option, as it was for nuclear weapons. Unlike nuclear weapons, the offensive capability of cyber is not limited to nation states. Any individual or group can go to a store, buy a computer, look on the internet for basic hacking tools, and begin practicing from any computer connected to the internet. Cyber deterrence is not just against another nation, but an entire spectrum to include criminal organizations, hackers, and state-sponsored groups. This is a major reason why a singular deterrent policy

would suffer across the cyber spectrum. The technology exists to spoof one's actual location and make it seem you are somewhere else. This creates problems when trying to attribute blame for the attack.[16] If you cannot accurately figure out who did it and why, you struggle to fight against it. The enemy becomes ill defined. By the time countries figure out where the attack originated, the damage may be done and any action taken will be too late for effective or timely retaliation. A future deterrence policy must be flexible enough to deal with all actors and the varied motivations.

A future deterrence policy must be flexible enough to deal with all actors and the varied motivations.

U.S. Department of State

In March 2016, the State Department published their International Cyberspace Policy Strategy. This strategy is based on "implementing the President's International Strategy and reflects three themes: the applicability of international law; the importance of promoting confidence building measures; and, the significant progress the Department has made…to promote international norms of state behavior in cyberspace."[17] These themes are, and have been, worked into diplomatic discussions with foreign nations. In 2015, the U.S. State Department secured the "G20 Leaders' commitments to affirm the applicability of international law to state behavior in cyberspace."[18] This commitment also endorsed norms of behaviors states should abide by.[19] These same commitments are part of the ongoing effort by the State Department to gain trust and voluntary buy-in from nations across the globe on additional measures.[20] It must be noted these future commitments are voluntary with risk being pushed aside until the next large global event. Much like 9/11 changed the nature of U.S. military commitments, the next event could set in motion a chain of events which cause any agreements not formalized in treaty or law to easily be discarded and new rules established. Credit is due to the U.S. for beginning to lay the framework of cyber stability as risks are highlighted by states employing cyber capabilities.[21] However, there is still much work needed to gain formalized treaties and write new international law. These efforts must continue in earnest until such a time as the international community comes to an agreement with respect to the entire span of cyber actions and actors. Nations using loopholes and new ways of getting around the agreements and letter of the law must be anticipated and expected. Formalized agreements with clear language are the best way to hold nation states accountable within the international community for offensive acts conducted in the cyber domain. Such agreements will deter other nations from engaging in the cyber domain as punishments will be articulated and actors can weigh the cost-benefit of using OCO weapons.

Conclusion

Cyberwarfare was not introduced to the world like the nuclear bomb, rather it has been gradually tested and its usage increased by organizations seeking to gain advantage over their adversaries. Though the potential strategic destructive power (predominantly temporary in nature) is similar to nuclear weapons with respect to a large area affected instantaneously, a deterrence strategy like MAD will not work due to the wide range of entities capable of conducting cyber-attacks. The U.S. deterrence strategy needs to be flexible enough to detract criminal organizations through judicial punishments, as well as state actors through sanctions ranging from economic to military action. There needs to be a defined and clearly articulated response if the U.S. were attacked by

a nation state, providing other states an expectation of the level of retaliation. Something akin to the escalation ladder concept used after World War II would work. This prevents an either/or situation, where if you don't act at all, your military credibility is damaged. A wide range of options allows a measured response to demonstrate the resolve to protect national interests, based on who and where the threat is coming from. The flexibility of an escalation ladder concept communicates to other nations they are on the ladder, on a path to larger conflict and gives them an opportunity to stop their actions before facing a greater response from the U.S. Additionally, any 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 would be in place only during times of peacetime operations. If two nations were to go to war, either a cyber war or a conventional shooting war, this ban would then be lifted.[22] 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, protects non-combatants, and prevents indiscriminate attacks, whether intentional or not.

Further, the international community needs to define what constitutes cybercrime and cyberwar in order for countries to develop clear strategies for OCO and deterrence. One cannot deter what is not defined! The definitions should start with the motivation of the group conducting the attack as well as the intended purpose of the attack, then build out from there. These definitions allow countries to seek appropriate justice within the international community rather than try and retaliate on their own. Pressure brought from the international community has the potential to do more to hold renegade actors in check and keep wars from beginning. These actions will allow the U.S. to more effectively deter cyberattacks and get ahead of nations who already employ cyber without regard to international norms. The U.S. must articulate a clear deterrence strategy in the cyber domain and lead the international community to an acceptable treaty signed by all nations limiting OCO against civilian targets. ***IAJ***

NOTES

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 Ibid.

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 Ibid.

7 Ibid.

8 Ibid.

9 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).

10 Ibid.

11 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).

12 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).

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

14 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).

15 Ibid.

16 Ibid.

17 U.S. Department of State, *International Cyberspace Policy Strategy*, 2016: 1-24. https://www.state.gov/documents/organization/255732.pdf

18 Ibid.

19 Ibid.

20 Ibid.

21 Ibid.

22 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).