LIBERTY UNIVERSITY

Liberty University Journal of Statesmanship & Public Policy

Volume 1 | Issue 2 Article 6

January 2021

Cyber Mutually Assured Destruction & Counterproliferation for the 21st Century: “How I stopped worrying and learned to love the software exploit.”

Peter R. Pattara
Liberty University

Cyber Mutually Assured Destruction & Counterproliferation for the 21st Century

In the twentieth century, the United States inherited the role of the British Empire and became a global geopolitical hegemon. In its quest to take on that mantle, the United States revolutionized geopolitical competition by developing nuclear weapons. The unique opportunities and challenges these weapons created took many years to integrate into strategic planning. This parallels the twenty-first century revolution of international competition through the introduction of cyberspace as a theater of competition. The development of the internet, and its inevitable weaponization, has presented the strategic community with an ongoing challenge. How can the United States integrate cyber threats into their strategic calculus? A solution may be found in the principles that nuclear strategy uses to deter and overcome threats. This paper will dissect the nuclear strategy to identify those principles, construct a framework for cyberspace integration, and make some policy proposals for implementation.

Strategic Nuclear Weapon Doctrine

The United States has two separate approaches in addressing nuclear threats. They are categorized by near-peer nation-states, which already possess nuclear weapons, and non-peers or non-state actors, who do not possess nuclear weapon capabilities. The differing strategies are colloquially referred to as Mutual Assured Destruction (MAD) and Counterproliferation. The principles of each, deterrence and survivability, and operational disruption or destruction can be seen through an examination of the strategy.

Near-Peers & Mutual Assured Destruction

It is important to consider that the United States unilaterally introduced nuclear weapons to the world by bombing Hiroshima and Nagasaki; however, this provided only a short-lived advantage since the nuclear arms race soon gave adversaries like the Soviet Union matching nuclear capabilities.[1] Such countries with matching capabilities are the near-peer states relevant to this discussion. MAD became the doctrine of choice against these states. In short, MAD deters nuclear conflict by ensuring a credible retaliatory capability exists, to make adversaries believe that their survivability value in the open conflict expression is nil. Originally proposed under the Eisenhower Administration, it was known as "massive retaliation," and was designed to deter Soviet aggression with the strategic goal of nuclear superiority.[2] For clarity, MAD proposed that since nuclear weapons were so destructive, their use must be prevented at all costs. Therefore, planners proposed that the United States and the Soviet Union must deter each other from employing such weapons. The best deterrent was thought to be ensuring that a survivable capability existed to retaliate and defeat the attacking party.[3] It is important to note that this policy was not simply diplomatic rhetoric; rather, it was credibly reinforced by armed force doctrine, technology, and forces.

Under President Eisenhower, strategic planners developed the Nuclear Triad of forces, including Strategic Air Command's bombers, Intercontinental Ballistic Missiles (ICBMs), and Submarine Launched Ballistic Missiles (SLBMs) to ensure the capability of American forces to

[1] David McDonough, "Nuclear Superiority or Mutually Assured Deterrence: The Development of the US Nuclear Deterrent," *International Journal* 60, no. 3 (2005): 812.

[2] Ibid, 812.

[3] Ibid, 814.

launch a retaliatory strike if nuclear war broke out.[4] The Triad provided a "second-strike" capability. Interestingly, the Soviets took this second-strike capability further and are alleged to have developed man-portable nuclear weapons, which the KGB First Directorate covertly deployed to Western nations for clandestine operatives to use if war broke out and the Soviet military were unable to launch their traditional nuclear capabilities.[5]

Counterproliferation Strategy

State Actors

The United States also utilized a complementary strategy towards nation-states which had not developed nuclear weapons. For states actively developing nuclear weapons, the United States' tool of choice has become known as counterproliferation, referring to the effort to physically, technically, and diplomatically prevent a state from obtaining nuclear capabilities. Several Military Mission Areas were developed for the Department of Defense: most notably, WMD Interdiction, Offensive Operations, and Elimination.[6] Under these operations, the United States would intercept materials to create nuclear weapons, eliminate development program nodes, or destroy a nuclear weapons program, not entirely dissimilar to the Israeli Operation OPERA which destroyed the Osirak nuclear reactor in Iraq.[7] For those states which were not actively seeking nuclear weapons, the United States employed a full range of activities, which included extensive intelligence gathering to detect attempts to proliferate, actions to dissuade potential suppliers, and enable allies for counterproliferation. Diplomatically, treaties and tools were drafted to allow peaceful engagement between states, with the Non-Proliferation Treaty (NPT) serving as a high-level illustrative example.

Non-State Actors

Not all nuclear threats come from nation-states; some non-state actors like terrorist organizations could potentially present a nuclear threat. The United States' counterterrorism forces accounted for such a contingency, and the counterproliferation policy was adapted in the 1980-90s to address the growing threat from terrorism.[8] The Joint Special Operations Command (JSOC) created the "0400" mission area to physically interdict against terrorist proliferation. JSOC assigned Special Missions Units (SMUs) including elements of Task Force Green/Combat Applications Group (TF-Green) and Task Force Blue/Naval Special Warfare Development Group (TF-Blue) to these mission sets. Elements from the SMUs were kept on ready alert to respond to and capture nuclear material or destroy terrorist nodes seeking nuclear material. To summarize, the United States adopted a posture of deterrence through MAD against peer nation-states and operational mission areas to disrupt smaller adversaries weapon acquisition efforts.

---

[4] Ibid, 814.

[5] Vasili Mitrokhin and Christopher Andrew, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999).

[6] Joint Chiefs of Staff, *JP 3-40: Joint Countering Weapons of Mass Destruction* (Department of Defense, 2019), I-3, B-3, B-6.

[7] Ibid, IV-4.

[8] Sean Naylor, *Relentless Strike: The Secret History of the Joint Special Operations Command* (St. Martin's Press: London, 2016).

Strategic Similarity Between Nuclear & Cyber

International competition in cyberspace shares significant similarity in a strategic sense with the nuclear arms race of the Cold War. The unilateral discovery of each technology and their destructive potential acts as an example. These similarities make a compelling justification for comparison and application of the lessons from nuclear weapon strategy.

Unilateral Technological Revolution

The initial versions of the internet took shape in the late 1960s with the Advanced Research Projects Agency Network (ARPANET), which laid the groundwork for the modern internet networks observed today. This technology changed the very nature of strategic competition by opening an entirely new theater of operations that was fundamentally different from any seen before.[9]

The weaponization of the internet, like the weaponization of nuclear fission, began with an American Special Access Program (SAP). For nuclear weapons, the United States had the Manhattan Project. In cyberspace, the United States began the program known as NITRO ZEUS.[10] The cyber Hiroshima was the deployment of a virus known as Stuxnet by NITRO ZEUS forces to destroy Iranian industrial Uranium enrichment facilities.[11] It is worth noting that open-source intelligence indicates that Stuxnet was developed under the NITRO ZEUS program, but the virus may have been launched by Israeli cyber forces who collaborated with the American National Security Agency on the program under another SAP codenamed OLYMPIC GAMES.[12] Despite this, the use of the virus can be considered the beginning of the cyber arms race similar to the Cold War nuclear arms race.

Destructive Capability

The destructive potential of cyberweapons should be explored and defined clearly. Cyberweapons themselves can range in destructive potential, from small and minimally destructive attacks to much larger attacks. It cannot be understated that offensive cyber operations can create physical degradation, disruption, or destructive effects.[13] Under NITRO ZEUS, the NSA's Tailored Access Operations unit penetrated Iranian cyber networks and implanted software exploits inside transportation, electrical, air defense, and military communication networks.[14] The exploits were designed to monitor activity and could activate on command to blackout the electrical grid, blind air defense networks, sabotage transportation, and silence military

[9] Joint Chiefs of Staff, *JP 3-12: Cyberspace Operations* (Department of Defense, 2018), IV-15.

[10] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Portland: Broadway Books, 2013).

[11] Ibid.

[12] Robert Cromwell, "Cyberwar – USA." *Cromwell Intelligence.* March 2018. https://cromwell-intl.com/cybersecurity/cyberwar/usa.html

[13] Benjamin B. Hatch, "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits", *Journal of Strategic Security* 11, no. 1, (2018): 45.

[14] David E. Sanger & Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times*, February 16, 2016, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

communication networks.[15] High impact malware could even be considered a weapon of mass destruction since they meet the characteristics of destructive design, mass casualty capability, and are considered special weapon systems.[16] In direct application to the United States, a cyber-attack on the American power grid could be economically and socially devastating. A Lloyd's of London threat assessment of such a strike estimated an economic loss in excess of $243 billion dollars[17] and substantial loss of life.[18] From these premises, it can be logically concluded that nuclear and cyberweapons are sufficiently similar, justifying the integration of cyberweapons into the weapon of mass destruction strategic framework.

Strategic Framework for Cyberweapons

Considering these nuclear strategy characteristics and the similarity between each technology, a logical approach may be to scale United States cyber response based upon the nature of each threat. To form a cyber framework, the nuances of near-peer states and other adversaries must be addressed. This framework ought to pursue the same general objectives of the nuclear strategy, in short, to prevent the use of such weapons, through deterrence, and spread of the weapons, via operational disruption.

Near-Peer States

Against near-peer state adversaries, the United States' objective ought to parallel the objective against nuclear threats. The comprehensive tools, diplomatic, intelligence, and military used against nuclear weapons retain strategic relevance. It is in the strategic interest of the United States to prevent conflict rather than simply prevailing to avoid the consequences. As Sun Tzu said:

> "Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting. The best victory is when the opponent surrenders of its own accord before there are any actual hostilities... It is best to win without fighting."[19]

The chief difficulty with any deterrence strategy using MAD is ensuring that a capability can credibly present a second-strike threat. Further, the strategy should avoid escalation to nuclear conflict. To accomplish this objective, this paper suggests two policy implementations to establish survivable cyber deterrence.

[15] Paul Szoldra, "The US could have destroyed Iran's entire infrastructure without dropping a single bomb," *Business Insider, July 6*, 2016, https://www.businessinsider.com/nitro-zeus-iran-infrastructure-2016-7.

[16] Hatch, "Defining a Class of Cyber Weapons as WMD," 44.

[17] Robert K. Knake, "A Cyberattack on the U.S. Power Grid," *Council on Foreign Relations*, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid.

[18] Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations," *International Committee of the Red Cross (ICRC)*, November 16, 2018, https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf.

[19] Sun-tzu, *The Art of War*, trans. Samuel Griffith, (Oxford: Clarendon Press, 1964).

Implanted Exploits

The United States could adopt a deterrence posture by developing implanted software exploits to be triggered as a second strike. This approach is like the Soviet tactic of smuggling nuclear devices into western nations covertly so clandestine agents could employ them against NATO targets. The technical viability of this strategy has been explored by the original NITRO ZEUS program in the Iranian context.[20] The exploits designed by the NSA against Iranian infrastructure could have been like weapons of mass destruction. Such exploits on systems like electric power or water purification could cause significant loss of life which would serve to raise the cost of conflict and therefore deter it. Open-source information indicates that the Russian Federation has undertaken cyber-attack measures against the United States' infrastructure, which could be intended for such a purpose.[21] Admittedly, this tool would provide only limited effectiveness since MAD requires a credible risk. Covert exploits cannot be openly acknowledged, lest the adversary disable them. Thus, credibility would be difficult to establish and the deterrent effect would be minimal.

Submersible Ship Data Nuclear (SSDN)

The United States could also design survivable cyber-attack infrastructure from which a second strike could be launched. This follows closely with the strategic thinking behind the submarine-launched ballistic missile programs which began early in the Cold War. Traditional data center architecture raises survivability concerns that a modified submarine design could mitigate. Naturally, such an architecture would raise infrastructure and connectivity challenges, but those can be mitigated in the design. Nuclear submarines have already necessitated the development of highly sophisticated cooling systems to regulate reactor core temperatures. These solutions could be applied to overcome the chief concern for data center servers, which is heat. Such a system could also utilize advanced terahertz frequency lasers to conduct ultrafast frequency modulation for frequency shifting high data-bit transmission to prevent jamming and backscatter attacks.[22] In a cyber strike contingency, the submarines could connect to land or satellite internet ports using the laser transmitters and launch retaliatory cyberweapons. It is worth stressing that this tool would not solve the challenges of identifying and attributing cyber-attacks, which are even more difficult due to obfuscation via dark or deep web networks.

Counter Cyber Proliferation

Against non-state actors or states, a modified counterproliferation strategy could be employed. It remains in the strategic interest of the United States to continue efforts to prevent the spread of highly technical cyberweapons like advanced persistent threats. A Counter Cyber Proliferation (CCP) strategy which includes diplomatic, intelligence, and military components, would mirror existing counterproliferation regimes. The military implementation would be a mission area dedicated to interdicting against adversaries developing cyber capabilities.

[20] Sanger & Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict."

[21] Hatch, "Defining a Class of Cyber Weapons as WMD," 49.

[22] Aniela Dunn et al., "High-speed modulation of a terahertz quantum cascade laser by coherent acoustic phonon pulses", *Nature Communications* 11, no. 835 (2020): 1.

Joint Special Operations Task Force - Cyber

This would require a dualistic approach utilizing traditional special mission forces to physically interdict nodes, destroying equipment, disrupting planning cycles, and detaining hostile actors. Such an approach would also involve similar mission areas in the cyber theater, for instance physically destroy threatening cyber infrastructure or capturing hostile cyber personnel. To this end, creating a JSOC task force to interdict and destroy cyberweapon program nodes and organizations would complement the existing task forces and provide a highly enhanced lethality to the DOD's counterproliferation mission. These missions would likely follow the F3EAD model (Find, Fix, Finish, Exploit, Analyze, Disseminate) refined by JSOC task forces throughout the Global War on Terror (GWOT). The most significant challenge to counterproliferation against cyber threats is the attribution of attacks and precursor activity especially through deep or dark web,[23] but existing capabilities are projected to resolve this issue.

Further, attribution was a challenge for JSOC during the GWOT, but it was largely solved through rigorous intelligence collection and interagency integration of intelligence collectors and networks into the kill chain. Intelligence professionals identified targets and armed forces personnel captured or eliminated the identified targets to spur further intelligence collection. Additionally, establishing a cyber-centric SMU under the JSOC operational umbrella could permit the command to conduct operations through cyberspace and integrate expertise. The same principle drove the establishment of TF-Green's Heavy Breaching Cell to overcome unique challenges presented by reinforced underground bunkers in counterproliferation missions.[24] These operational moves could improve strategic posture and prevent further hostile cyberweapon development. Though outside this paper's scope, diplomatic planners should also consider the proposition of emulating the NPT in a cyber context to formalize permitted and non-permitted scientific and technological research or regulating advanced computing capabilities like quantum computing with enforcement and monitoring mechanisms reminiscent of the NPT.

Conclusion

The United States faces growing challenges in the international community. The peace dividend following the collapse of the Soviet Union was expected to bring about a lasting, peaceful world order. Instead, global anarchy has increased. The world of cyberspace has opened the United States to previously untold avenues of attack. This has challenged the strategic calculus and created much fear in the American public. However, such situations have been resolved before. Similar strategic disruptions occurred following the development of the nuclear bomb. The United States adopted a strategic posture to deter peers from using nuclear weapons and disrupt proliferation of nuclear weapons to non-nuclear states. The nuclear strategy can serve as a model for adapting to the threats from cyberspace. Deterring near-peer adversaries and countering cyberweapon development programs within a novel framework can improve the United States' national security posture and better protect its citizens. Of additional importance are diplomatic policies, like proposing a cyber non-proliferation treaty, but they remain outside the scope of this paper and may be an appropriate area for future research and consideration.

[23] Office of the Director of National Intelligence, *A Guide to Cyber Attribution: Leading Intelligence Integration* (Washington, D.C.: ODNI, 2020).

[24] Naylor, *Relentless Strike*, 107.

Bibliography

Cromwell, Robert. "Cyberwar – USA." *Cromwell Intelligence,* March 2018, https://cromwell-intl.com/cybersecurity/cyberwar/usa.html

Dunn, Aniela, Caroline Poyser, Paul Dean, Aleksandar Demic, Alexander Valavanis, Dragan Indjin, Mohammed Salih, et al. "High-speed modulation of a terahertz quantum cascade laser by coherent acoustic phonon pulses." *Nature Communications* 11, no. 835 (2020). https://doi.org/10.1038/s41467-020-14662-w.

Hatch, Benjamin B. "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits." *Journal of Strategic Security* 11, no. 1 (2018): 43-61. https://doi.org/10.5038/1944-0472.11.1.1657.

Gisel, Laurent, and Lukasz Olejnik. "The Potential Human Cost of Cyber Operations." *International Committee of the Red Cross (ICRC),* November 16, 2018. https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf.

Joint Chiefs of Staff. *JP 3-12: Cyberspace Operations*. Washington, D.C.: Department of Defense, June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

_____. *JP 3-40: Joint Countering Weapons of Mass Destruction.* Washington, D.C.: Department of Defense, November 27, 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_40.pdf.

Knake, Robert. "A Cyberattack on the U.S. Power Grid." *Council on Foreign Relations,* April 3, 2017. https://www.cfr.org/report/cyberattack-us-power-grid.

McDonough, David S. "Nuclear Superiority or Mutually Assured Deterrence: The Development of the US Nuclear Deterrent." *International Journal* 60, no. 3 (September 2005): 811–23. https://doi.org/10.1177/002070200506000314.

Mitrokhin, Vasili, and Christopher Andrew. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 1999.

Naylor, Sean. *Relentless Strike: The Secret History of Joint Special Operations Command*. London: St. Martin's Press, 2016.

Office of the Director of National Intelligence. *A Guide to Cyber Attribution: Leading Intelligence Integration*. Washington, D.C.: ODNI, 2018. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

Sanger, David. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Portland: Broadway Books, 2012.

Sanger, David E., and Mark Mazzetti. "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict." *The New York Times*, February 16, 2016. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

Sun-tzu. *The Art of War*. Translated by Samuel B. Griffith. Oxford: Clarendon Press, 1964.

Szoldra, Paul. "The US could have destroyed Iran's entire infrastructure without dropping a single bomb." *Business Insider*, July 6, 2016. https://www.businessinsider.com/nitro-zeus-iran-infrastructure-2016-7.