AIR WAR COLLEGE

AIR UNIVERSITY

# REALITIES OF DETERRENCE AND RETALIATORY OPTIONS TO ATTACKS IN SPACE AND CYBERSPACE

by

Shawn C. Fairhurst, Colonel, USAF



A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 February 2012

## Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

# Biography

Colonel Shawn Fairhurst is a US Air Force space and missile operator assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from the United States Air Force Academy in 1990 with a Bachelor of Science degree in Aeronautical Engineering, and Troy State University in 1997 with a Master of Science degree in Management. He has extensive space and missile expertise including satellite command and control, ICBM operations, and overhead persistent infra-red satellite operations. He has held positions at the wing, NAF, center and MAJCOM levels and is a graduated squadron commander.

## Abstract

Since the last years of the 20th Century, threats in space and cyberspace have become prominent, to the point where an attack can threaten state sovereignty and have regional, if not global consequences. These threats are emerging at the same time that the United States' reliance on its own space and cyber capabilities increases to maintain international diplomatic leadership and conventional military superiority. US national policy speaks to deterring and defending against such attacks, but a lack of international precedent and the legal limitations of war, specifically attribution, proportionality and discrimination, limit United States response options to an unprovoked attack in these domains. In order to establish an effective deterrence, the United States must move away from the Cold War model and fashion a global environment that fosters effective deterrent strategies. Building this new order requires the United States lead the international debate to define attacks in space and cyberspace and appropriate "self-defense" responses under Article 51 of the United Nations Charter. The United States must demonstrate the political will to take action unilaterally, if necessary, to set precedent, and erase the failures of past transgressions, including NATO's failure to respond to the Estonia cyber attacks in 2007. As deterrence is predicated on the ability to attribute in order to hold an adversary at risk, the United States must improve its ability to detect and attribute attacks in space and cyberspace. Finally, the United States must reduce its space and cyberspace vulnerabilities and prove to any potential adversary that its military can successfully fight through any degradation and win. Unless the United States takes prominent actions on these fronts and establishes an international recognized lexicon on space and cyberspace, any deterrent posture will likely fail and it will remain at risk to asymmetric attacks by adversaries emboldened by a veil of anonymity, who see the benefits of attacking the United States outweighing the risk of an unprovoked first strike.

# Introduction

"*Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur…. This new character of war, emphasizing the advantages of the offensive, will surely make for swift, crushing decisions on the battlefield…. Those who are ready first not only will win quickly, but will win with the fewest sacrifices and the minimum expenditure of means."* Giulio Douhet (1921)[1]

Douhet's description of airpower is applicable today as the United States addresses modern warfighting challenges in the space and cyberspace domains. Over the last decade, actions by nation states and non-state entities have blurred the lines between these domains and opened the world's eyes to a new emerging threat. Hackers have taken control of government owned satellites, nations have developed and proven antisatellite capabilities, sovereign governments have been victims of cyber attacks and computer viruses have become potential instruments of power. It is an evolving landscape of electronic and kinetic threats that may merely scratch the surface of what might be at an adversary's disposal to threaten US conventional military superiority and national sovereignty.

Through national policy and international engagement, the United States has established its right to defend its access and assets from attack in space or cyberspace and is engaged in vigorous debate to define strategies to deter such attacks. However, as the seams between US space and cyber capabilities close, the realities of conflict in space and cyberspace, including international laws and norms, the difficulties of attribution and discrimination, and the risk of escalation, conspire to undermine credible deterrence and limit retaliatory options following an attack.

## Characterizing the Asymmetric Threat

"*In the information age, the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker."* Qiao Liang and Wang Xiangsui[2]

Vital US infrastructures supporting business, government, defense and emergency response rely upon a network of space and cyber systems that are intricately linked; each domain reliant upon the other as part of the overall network.[3,4] As reliance grows, so does the threat of attack from potential adversaries who recognize a potential "Achilles' heel" in US military dominance, with recent events exposing how the threats within space and cyberspace have evolved:[5]

- Hackers have bridged the gap between space and cyberspace. In 1999, hackers reportedly took control of a British Defense Ministry communications satellite; and in 2008, during two separate attacks, hackers accessed National Aeronautics and Space Administration (NASA) telemetry, tracking and control (TT&C) systems and gained full control of two US Earth imaging satellites. [6,7]
- Kinetic-attack antisatellite (ASAT) capabilities were demonstrated for the first time in two decades. On 17 January 2007, China successfully launched an ASAT that destroyed an inactive Chinese weather satellite in an orbit similar to US and other nations' imagery and intelligence satellites.[8]
- In April 2007, a distributed denial-of-service (DDOS) attack targeted Estonia's financial and government agencies, crippling its communications infrastructure and represented the "first explicit large-scale computer attack for political rather than economic purposes."[9]
- The DDOS attacks launched by civilians and Russian crime gangs against the Republic of Georgia in the summer of 2008 brought internet traffic to a standstill within the country and are the first known cyber attacks that coincided with a shooting war.[10,11]

- The world may have seen its first cyber weapon. The Stuxnet worm discovered in June 2010 appears to have been specifically designed to attack Iran's nuclear program by destroying the centrifuges used to enrich uranium.[12]

Recent history and the intertwining of space and cyberspace capabilities only begin to characterize the myriad potential threats that are of concern for US national security. With a deepening reliance on space and cyberspace systems and insufficient effort to reduce vulnerabilities, the United States is enticing adversaries to research options from kinetic attacks to cyber attacks that may enable a crippling asymmetric "first-strike."[13,14] These factors are driving the United States to issue policies and evaluate strategies in an attempt to assure both its access and the security of its assets in both domains.

## US Policy and Realities of Space and Cyberspace Deterrence

Current US policy recognizes that our world's increasing reliance on interconnected and networked capabilities poses security challenges where acts by irresponsible and malevolent actors in space and cyberspace have damaging consequences for everyone, to include endangering international peace.[15,16] Consistent with Article 51 of the United Nations (UN) Charter, the United States maintains the right of self-defense in response to aggressive acts in space and cyberspace.[17,18,19] US national security policy seeks to deter, defend against and, when required, defeat efforts to interfere with United States' and its allies' efforts in space and cyberspace and hinges upon strategies that convince an adversary that the risks associated with attacking in space or cyberspace greatly outweigh any potential benefits.[20,21]

This focus on "convincing an adversary" through deterrence is likely rooted in the fact that the United States has limited ability to improve its space and cyberspace defenses and effectively mitigate existing vulnerabilities.[22] The nuclear deterrence model that dominated the

Cold War was built upon a foundation much different than that existing in space and cyberspace. For 60 years the United States pursued deterrence through the "principle of retaliation in kind," mutual assured destruction, a strategy forged by the view that state survival was paramount and nuclear war was unacceptable and to be avoided.[23,24] Deterrence between the United States and the Soviet Union was bi-polar, between known adversaries. This is not the case today, as individuals, criminals, terrorists, non-state and state actors may all possess capabilities that could negatively impact US conventional superiority by exploiting its space and cyberspace vulnerabilities.[25]

Effective deterrence "discourages an opponent from committing an act of aggression by manipulating the expectation of resultant costs and benefits." [26] The ability of the United States to establish a credible deterrent posture in space and cyberspace depends on four key components: the ability to detect an attack; the capability to attribute who is responsible; the ability to inflict an appropriate cost to the attacker; and a communicated conviction to any aggressor that the United States has the political will to retaliate.[27,28] These components are the foundation to justify for a retaliatory response and exist in a nexus of international law, presenting unique challenges across the space and cyberspace domains:[29]

- First, deterrence requires understanding what is being deterred and a forceful response is justified as the result of an attack. Therefore, the United States must establish, characterize and define what constitutes an attack in these domains.
- Second, the ability to identify both the adversary you want to deter and who executed an attack is essential and necessary under international law and custom to justify a response in self-defense. However, in space and cyberspace, establishing culpability is difficult.

- Third, deterrence implies the ability and political will to retaliate to inflict an appropriate cost on a perpetrator of an attack in space or cyberspace. The right to respond, and therefore hold an adversary at risk, is determined through precedent and governed by the concepts of proportionality and discrimination.
- Finally, retaliatory options require an evaluation of perceived risks and benefits to both sides and may negatively influence US political will to forcefully respond following an attack in these domains.

## Defining an "Act of Force" in Space and Cyberspace

Currently, there are no universally recognized definitions of an "act of force" in space and cyberspace as attacks in both domains run the spectrum from nuisance to destructive. While a kinetic attack in either domain would likely qualify as an "act of force," each act, especially those that do not cause human death or destruction of property, must be assessed individually to determine if an "armed attack threshold" was crossed, constituting a use of force.[30] Without crossing this "use of force" threshold, justifying a forceful response is problematic under international laws and norms.

It is easy to make an analogy that an attack in space or cyberspace is "like" an attack in a different domain that would be considered an act of war; however, without an internationally accepted framework, it is difficult to defend this position.[31] At the macro level, it is possible to generalize that space or cyberspace attacks causing physical damage, injury or death, are on par with traditional acts of war, and therefore would qualify as a use of force and an armed attack. It could also hold then, that attacks resulting in repairable damage, no long-term consequences and no injury to humans would likely not be seen as having crossed the threshold of a use of force and armed attack.[32]

In their book *Cyberpower and National Security*, the authors explain the seven factors of Professor Michael Schmidt's framework to determine whether a cyber attack crosses the threshold of an illegal act of armed force.[33] As the space and cyber domains are intricately linked and attacks in one may impact or transit the other, this framework also holds well to evaluate attacks in the space domain.

- Severity: Addresses scope (area), intensity (damage done) and deaths.[34]
- Immediacy: Addresses how quickly the attack occurs, its duration and how long effects remain.[35]
- Directness: Addresses if the action is distinguishable from other parallel actions and if the effects felt are directly caused by the action.[36]
- Invasiveness: Addresses whether the action violates a country's physical border and if the locus of the action is within the target country.[37]
- Measurability: Addresses the certainty of how quantifiable the effects of the attack are and how distinguishable they are from other actions' effects.[38]
- Presumptive Legitimacy: Addresses the actions' legitimacy through precedent within the international community and qualitative similarity to actions presumed legitimate under international law.[39]
- Responsibility: Determines if the action is directly or indirectly attributable to the acting state, and if not for the acting state, that the action would not have occurred.[40]

Retaliation is normally a response to an attack that causes damage or pain.[41] Currently, definitive guidance on attacks in space and cyberspace has not been established by the UN, a large alliance such as NATO, or through international court decisions. Establishing an internationally recognized framework will enable nations to pursue effective deterrence

strategies to prevent aggression in space and cyberspace while helping to legitimize a nation's claim that it has sustained an attack.[42] However, unless a nation can identify the source of an attack, any deterrent strategy or threat of response is "without teeth" and renders forceful retaliatory actions illegal.

## Attribution in Space and Cyberspace

Unlike nuclear deterrence, attackers in cyberspace, and in many instances in space, have the advantage due to the ability to conceal their identities.[43] Recent examples expose the difficulty in attributing actions in space and cyberspace:

- The cyber attack on Estonia was largely believed to be authorized by the Russian government, but no evidence directly linked the attacks.[44]
- The hacking of the US land-imaging satellites in 2008 was widely conjectured as a Chinese action; however, these incidents were never publicly attributed to an attacker.[45]
- The Stuxnet worm is widely thought to be an Israeli cyber attack, supported by the United States, but counter theories exist and no one has established definitive responsibility.[46]

This anonymity can build the attacker's confidence and weaken any deterrent strategy, mitigating the risk of retaliation by force.[47]

Attribution and "first-strike instability" are compounded by limitation in the ability of the United States to maintain both space situational awareness (SSA) and cyberspace situational awareness (CSA). SSA is limited by the fact that the United States cannot monitor all its satellites constantly nor maintain 100 percent coverage of the domain. This lack of coverage makes diagnosing the cause of a sudden failure difficult as the United States may not be able to determine whether the cause is environmental (e.g., micrometeorite, solar flare, debris) or by attack (e.g., kinetic, directed energy, TT&C hack).[48] Total CSA is improbable and it is doubtful

that a network can be completely secured from attack, given new viruses are created constantly and new software and humans in the loop introduce unknown vulnerabilities that can be exploited as seen with the Stuxnet worm.[49]

In cyberspace, attribution is made more difficult by actors who may not even exist in the physical world, aren't constrained by geography or borders, and may launch an attack and quickly disappear. Creating a definitive link between a physical entity and a cyberspace actor is often an impossible tasking.[50] The Stuxnet code included references to both the hacker and his group; however, in cyberspace identities can be "spoofed" and code can be designed to implicate another to conceal the attacker's true identity.[51]

These factors also provide the United States with the benefit of anonymity for its actions in space or cyberspace. However, to establish credible deterrent strategies or justify overt forceful retaliation, the United States must convince the world of its ability to unambiguously attribute any attack in space or cyberspace to the right aggressor. Equally difficult is communicating a credible retaliatory threat given the lack of existing precedent and constraints outlined by international law and norms.[52]

## Governing Retaliatory "Use of Force"

Article 51 of the UN Charter specifically outlines a state's right to exercise self-defense in response to an armed attack, and since 1947, there has been much historical precedent governing the use of force for self-defense.[53] In 1974, the UN added that "states falling victim to terrorist attack from a country harboring or supporting the terrorists, could invoke the right of self-defense" as "involvement is equivalent to an armed attack."[54] Historically, the United States has exercised the right of self-defense with limited responses to isolated terrorist attacks:

- In 1986, following the state-sponsored bombing of a Berlin nightclub which killed two and injured 230 others, the United States launched a preemptive attack against Libyan leadership and terrorist facilities.[55]
- In 1998, the United States launched cruise missiles against terrorist compounds in Afghanistan and a chemical weapons factory in Sudan in retaliation for the earlier bombing of US embassies in Kenya and Tanzania.[56]

As no member of the UN Security Council objected to these actions, the United States established legitimacy for use of military action as self-defense against some terrorist attacks, broadening the interpretation of Article 51.[57]

Based on this broadening of the right of self-defense, it could be expected that the right of self-defense would apply to attacks in space and cyberspace, including those taken by non-state actors, or supported or endorsed by a sovereign state. Despite this analysis, no precedent exists for states exercising the right of retaliatory self-defense following an attack in these domains. Without precedent, deterrence and legitimacy for retaliation is difficult to establish.

## Precedent

Since the beginning of the space race, there has been discussion and international policy developed on the use of weapons in space. The 1967 Outer Space Treaty (OST) specifically addresses "demilitarized" celestial bodies and bans weapons of mass destruction in outer space.[58] However, there is no equivalent international agreement or policy governing the use of conventional weapons in space.[59] Instead, actions by the international community have set some precedence and established legitimacy for some "attack" capabilities within the space domain.

The Chinese ASAT demonstration in 2007 was a watershed event as no OST signatory attempted to enforce Article IX regarding harmful interference. [60] While the United States

publicly protested the Chinese actions, it demonstrated an ASAT capability in 2008 using its missile defense system. Further implying a proliferation of ASAT capabilities, both China and India demonstrated antiballistic missile capabilities in 2010.[61] The international community's failure to enforce the provisions of the OST or hold China (and subsequently the United States and India) accountable through policy or sanctions for their ASAT demonstrations has, in effect, established legitimacy for a state to possess the capability.[62] With regard to cyberspace, no such precedence exists.

As discussed earlier, few nations or international institutions have defined what constitutes an attack in cyberspace and no precedent governing the response that an attacker could expect in retaliation for an unprovoked attack has been established.[63] In 2007, despite one of its member nations, Estonia, being under cyber attack, NATO did not invoke its collective-defense clause. NATO's inaction missed an opportunity to establish a legitimate definition of an actionable attack in cyberspace and its lack of response failed to set precedence that could help deter other potential aggressors.[64] Additionally, the lack of US precedent for detection, attribution, and response, compounds the credibility of deterrence and threats of retaliation and may convince potential aggressors that an attack may not even elicit a retaliatory response.[65] However, when identified, an actor who initiates a "high-end" attack against the United States in space or cyberspace should expect that any retaliatory response need not be limited to the domain of the attack.[66] Before the United States could initiate such a response, it must address the requirements of proportionality and discrimination.

## Proportionality and Discrimination

Each unique attack requires a unique response and the concept of proportionality helps a nation determine an appropriate level of retaliation in response to an attack. Proportionality is an

internationally recognized legal restraint on the forceful actions a state may execute in response to an attack, reducing the violence and destruction to the minimum required to meet the objective—in simplified terms, the "use of force to defend oneself must not be excessive" and the "cost of the war must not outweigh the benefits."[67]

In the case of self-defense, a state's response is normally "proportionate to the injury being forcibly inflicted" in the initial attack.[68] To put into context, a jamming attack on a satellite that is reversible and does no damage would justify punishment on scale greatly reduced from a cyber attack that causes the destruction of a major power grid or the death of hundreds of people.[69] However, in cases of sustained individual attacks, the series of attacks can be evaluated as a whole and a disproportionate response to each individual attack may be taken in self-defense against the whole, and beyond the geographical confines of the initial attacks if decisive defensive action is necessary.[70]

The concept of proportionality is easily applicable in space and cyberspace domains, leading the United States to determine an "in kind" response is appropriate following an attack. However, "out of kind" kinetic responses against ground targets would likely fail the proportionality test, as "kinetic measures may be precise but generally not precise enough to get the proverbial terrorist-with-a-keyboard without doing considerable collateral damage. Moreover, it can be argued that the prospect of taking life in a kinetic attack far outweighs the damage one can commit with a cyber attack; that is, it is disproportional."[71] In the end, "it can be argued that [taking a life] far outweighs the damage [caused by] a cyberattack [sic]" and suggests that if proportionality will not hold, neither will discrimination if the US retaliates by invading a sovereign nation or causing human casualties when the aggressor's initial attack did neither.[72]

The concept of discrimination is two-fold in that it prohibits "direct and intentional attacks on noncombatants" and, under international law, any "foreseen" secondary effects on non-combatants due to an attack on a legitimate military target must be proportional to the military objective of the attack.[73] It is under the concept of discrimination that retaliation for a space or cyber attack meets an ethical roadblock. Space and cyberspace retaliation have the potential of causing unexpected second- and third-order effects, resulting in unintended and undesired consequences.[74] For example, kinetically attacking a satellite in response to an ASAT attack would generate thousands of pieces of debris, jeopardizing any satellite that transits the debris field. Likewise, a virus launched in cyberspace may not simply attack the intended target, as seen by the Stuxnet worm and its effects on systems worldwide not associated with Iran's nuclear program.[75]

As the majority of space and cyber assets are dual-use, the impact to non-combatants will likely outweigh the military objective, causing "in-kind" responses to fail the concept of discrimination. If this is the case, it is also unlikely the United States would retaliate in a different domain as some have suggested.[76] The factors of precedent, proportionality and discrimination all conspire against developing a credible deterrence and would likely cause the United States to pause in determining a retaliatory response and probably bolster the political will of an adversary, while simultaneously increasing the risk of escalation should the United States decide to retaliate through force.

## Political Will and the Risk of Escalation

The credibility of any US deterrent posture rests with the political will to carry out the promised retaliation; it is signaling to a potential adversary to influence his "risk versus return" calculus. However, it is more than simply convincing an adversary that the cost of his action

will outweigh the benefits. An adversary "weighs the perceived benefits and costs of a given course of action *in the context of* their perception of how they will fare if they *do not* act. Thus, deterrence can fail even when competitors believe the costs of acting will outweigh the benefits of acting—if they *also* believe that the costs of continued restraint would be higher still."[77]

As discussed, potential adversaries fully understand that the US military's qualitative advantage is significantly enhanced by its capabilities in space and cyberspace. The difficulties in securing systems in space and cyberspace, despite claims to the contrary, likely influence an aggressor's calculus that attacking US space and cyberspace systems offers a substantial benefit, as even limited success against a few high-value targets may provide substantial warfighting benefits.[78] Bolstered by a perceived shield of anonymity, an aggressor has even more positive indicators that an attack in these domains would be successful and it is likely that an aggressor who attacks the United States in space or cyberspace is not interested in controlling any unintended consequences; rather, he may be counting on them.[79]

Following such an attack, the United States will likely be focusing on more critical items than retaliation, such as:

- Determining whether war is imminent and with whom;[80]
- Based on the assessment of pending conflict, recovering defensive (and offensive) military capabilities lost in the attack, and signaling US readiness to respond to the pending attack;[81] and
- Responding to the needs of the American public, if the act directly caused pain and suffering or loss of critical infrastructure.

Only after addressing these will the United States begin planning for retaliation. Before the United States takes military action in response to a space or cyber attack, it must establish

accountability and attempt to determine the intent of the attacker. Without these components, any response may be misinterpreted, risking an escalation that could potentially spill into the physical terrestrial domains. The United States must decide if a "tit-for-tat" response would likely work to an adversary's advantage, especially with another state who may believe it has less to lose than the United States.[82]

When the concepts of proportionality and discrimination are included, US political will to respond to an attack in space or cyberspace may be further degraded. When dealing with assets and information removed from the public eye, "what credibly can be placed at risk that would dissuade a state [or other non-state aggressor] from contemplating such an attack? Presumably, the [United States] values lives more than bits, so any [kinetic] retaliatory threats are not credible," as the United States would likely lack the political will.[83] "The dilemma is more simply framed as a 'bits-for-lives' trade-off, in which the value placed on the challenger's life is always higher than the value placed on the defender's bits."[84] It is about perception, as "what one nation considers a 'cyber attack' might appear more like a 'cyber war' to another or even a simple 'cyber crime' to a third."[85]

## Recommendations

In order to build an international environment that will enable the development of credible strategies to deter attacks in space and cyberspace, the United States must address four key areas:

- Demonstrate political will and drive international policy.
- Develop improved situational awareness capabilities to attribute an attack.
- Establish precedent by using its hard and soft power to hold aggressors accountable for their actions in space and cyberspace.

- Mitigate its technical vulnerabilities and ensure the capacity to maintain conventional superiority in a degraded space and cyberspace environment.

The United States must demonstrate its resolve to the world that it considers its space and cyberspace assets as sovereign and vital to its national security interests.[86] It must communicate that any initiation or threat of counterspace or counter-cyberspace activities may be "viewed as more than a regional issue," likely impacting the global community, and "therefore, elicit an escalated US response."[87] This US perception that space and cyber attacks are an escalation of a conflict will provide better justification for its position that any response "need not be limited to a response in kind."[88] The political will to communicate this position will provide credibility to any US deterrent strategy and lay a foundation to engage the international community to establish accepted norms in space and cyberspace.

This demonstration of political will enables an integrated strategic communications plan to guide US diplomatic and information efforts. Through engagement with allies in NATO and the international community through the UN, the United States must lead the debate and establish norms that define illegal acts, ranging from crimes to armed attacks, in space and cyberspace. These internationally recognized norms would provide a foundation of stability in space and cyberspace, enabling a credible deterrence. Additionally, "fortifying taboos against attacking space [and cyberspace] assets would strengthen deterrence in another important way [by improving] the credibility of US threats to punish any state that violated the norm."[89] However, a lack of norms cannot hinder the US ability to respond to attacks in space and cyberspace. To enable a unilateral response, the United States needs improved capabilities to attribute attacks through the pursuit of improved situational awareness in these domains.

Credible deterrence and retaliation require attribution and the current lack of precedent involving US detection, attribution and response to attacks could embolden potential attackers.[90] To define credible deterrent postures and retaliatory responses, the United States must strive to understand an adversary's intents and improve its capabilities to identify threats, recognize attacks and establish culpability.[91] The United States must be able to deter and defend its "national security assets regardless if an attack is launched" by a sovereign state, non-state actors (e.g., mercenaries, criminal or terrorist organizations) or individuals with a political agenda.[92] With improved attribution the United States must then lead the international response if one is not present.

Whether or not international standards exist, if the United States identifies and attributes transgression in space and cyberspace, it must engage the international community through both NATO and the UN Security Council to apply pressure (both diplomatic and economic) and, when necessary punish (via military response) those who support, encourage and execute illegal acts in space and cyberspace.[93,94] If unable to achieve international engagement or multilateral support via its allies, it must still take unilateral action against the transgressor, consistent with existing international laws, in order to establish precedence that furthers US deterrent credibility.[95,96] Even if the United States displays strong political will, works to establish international norms, develops the ability to attribute attacks and leads the efforts to establish precedent, without addressing its own vulnerability, it still exposes itself to undue risk of attack.

To further deterrence credibility, the United States must erase the perception that its reliance on space and cyberspace capabilities presents asymmetric opportunities which may entice an aggressor's attack. It must "pursue multiple avenues to make vulnerable US space [and cyberspace] systems more resilient and defendable, thereby demonstrating tangible capabilities

to deny potential adversaries the benefits of attacking."[97] The United States must act overtly and consistently to convince any aggressor that it can continue to dominate on the conventional battlefield, despite degradation of its space and cyber capabilities.[98] It must learn to fight through these degradations while still prosecuting any conflict at the timing and tempo it desires; to do otherwise will give the advantage to the adversary.[99] Additionally, the United States must mitigate threats in cyberspace through defense in depth and the securing of its vital infrastructures that an aggressor may consider easy targets.[100] Any effort to establish deterrence or enable retaliatory options is the ability to fight through all phases of conflict and more importantly convince the enemy of this capability.

## Conclusion

The United States faces many challenges in developing effective deterrent strategies and retaliatory options for space and cyberspace. Adversaries emboldened by probable anonymity may see asymmetric attacks on US space and cyberspace capabilities as a beneficial course of action. Historically, the US precedent is to respond to small attacks with an overt limited response, yet the unique nature of space and cyberspace offers opportunities and challenges. Like a potential adversary, the United States could pursue a covert retaliatory response; however, this is a course the United States is unlikely to pursue given the greater risks to the United States in the event of uncontrolled escalation. Instead, the United States must use all its power to change the space and cyberspace landscape and cultivate an environment where credible deterrence and retaliatory options can exist. The United States must engage the international community to drive policy, establish precedent, reduce vulnerability and hold transgressors accountable. Given the United States and western world's reliance on space and cyberspace capabilities, these unresolved shortfalls will continue to undermine any deterrence strategies and

limit retaliatory options. Without US leadership to address these issues, the initiative and advantage will belong to the adversary.

# Bibliography


Beidleman, Scott W. "Defining and Deterring Cyber War." *Defense Technical Information Center*. US Army War College. June 1, 2009. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA500795 (accessed Oct 23, 2011).

Carr, Jeffrey. "British Nuclear Power Plant Goes Dark: Stuxnet Worm to Blame?" *Forbes.* November 1, 2010. http://www.forbes.com/sites/firewall/2010/11/01/british-nuclear-power-plant-goes-dark-stuxnet-worm-to-blame/ (accessed October 13, 2011).

—. "Did the Stuxnet Worm Kill India's INSAT-4B Satellite?" *Forbes.* September 29, 2010. http://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/ (accessed October 13, 2011).

—. *Stuxnet's Finnish-Chinese Connection.* December 14, 2010. http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/ (accessed November 27, 2011).

"Charter of the United Nations and Statute of the International Court of Justice." San Francisco: United Nations, 1945.

Cheng, Dean. "China's Space Program: A Growing Factor in US Security Planning." *Backgrounder*. Washington D.C.: The Heritage Foundation, August 16, 2011.

Chilton, Kevin and Greg Weaver. "Waging Deterrence in the Twenty-First Century." *Strategic Studies Quarterly* (Air University Press), no. Spring (2009): 31-42.

Coleman, Kevin. *Satellites could come under cyber seige.* September 22, 2010. http://defensesystems.com/articles/2010/09/02/digital-conflict-cyber-threat-to-satellites.aspx (accessed October 19, 2011).

*Cyberpower and National Security*. Dulles: Potomac Books, Inc, 2009.

Douhet, Giulio, Joseph Patrick Harahan, and Richard H. Kohn. *The Command of the Air*. Tuscaloosa, AL: The University of Alabama Press, 2009.

Farwell, James P. and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* (Routledge) 53, no. 1 (Jan 2011): 23-40.

GlobalSecurity.org. *Chinese Anti-Satellite Capabilities.* Unknown Unknown, Unknown. http://www.globalsecurity.org/space/world/china/asat.htm (accessed October 13, 2011).

Goodin, Dan. *Georgian cyber attacks launched by Russian crime gangs.* August 18, 2009. http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/ (accessed December 6, 2011).

Harknett, Richard J., John P. Callaghan, Rudi Kaufmann. "Leaving Deterrence Behind: War-Fighting and National Cybersecurity." *Journal of Homeland Security and Emergency Management* (The Berkely Electronic Press) 7, no. 1 (2010): Article 22.

*International Strategy for Cyberspace.* US Strategy, Washington D.C. : White House, 2011.

Johnson-Freese, Joan. *China in Space: Not Time for Bright, Shiny Objects.* July 1, 2011. http://defense.aol.com/2011/07/01/chinas-in-space-not-time-for-bright-shiny-objects/ (accessed December 9, 2011).

Laasme, Haly. "Estonia: Cyber Window into the Future of NATO." *Joint Forces Quarterly,* no. 63 (2011): 58-63.

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica: RAND, 2009.

Markoff, John. *Before the Gunfire, Cyberattacks.* August 13, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed December 6, 2011).

McIntyre, Jamie & Reuters. "CNN - US Missiles Pound Targets in Afghanistan, Sudan - August 20, 1998." *CNN.com.* August 20, 1998. http://edition.cnn.com/US/9808/20/us.strikes.01/ (accessed October 13, 2011).

McMillian, Robert. "Iran was prime target of SCADA worm - Computerworld." *Computerworld.* July 23, 2010. http://www.computerworld.com/s/article/9179618/Iran_was_prime_target_of_SCADA_worm?taxonomyId=85 (accessed October 13, 2011).

Morgan, Forrest E. *Deterrence and First-Strike Stability in Space.* Project Air Force, RAND, Santa Monica: RAND, 2010.

*National Security Strategy.* National Policy, Washington, D.C.: White House, 2010.

*National Space Policy of the United States of America.* US Policy, Washington D.C.: White House, 2010.

Pavlischek, Keith. "Proportionality in Warfare." *The New Atlantis: A Journal of Technology and Society* (Ethics & Public Policy Center), 2010: 21-34.

Qiao, Liang and Wang Xiangsui. "Unrestricted Warfare." *C4I.org.* Beijing: PLA Literature and Arts Publishing House. February 1999. www.c4i.org/unrestricted.pdf (accessed December 6, 2011).

Reagan, Ronald. "Address to the Nation on the United States Air Strike Against Libya." *Ronald Reagan Presidential Library Archives.* April 14, 1986. http://www.reagan.utexas.edu/archives/speeches/1986/41486g.htm (accessed October 13, 2011).

Ryan, Jason. *US Satellites Compromised by Malicious Cyber Activity.* November 16, 2011. http://abcnews.go.com/blogs/politics/2011/11/us-satellites-compromised-by-malicious-cyber-activity/ (accessed December 6, 2011).

Stark, Holder. *Mossad's Miracle Weapon--Stuxnet Virus Opens New Era of Cyber War.* August 8, 2011. http://www.spiegel.de/international/world/0,1518,778912,00.html (accessed December 11, 2011).

Sterner, Eric. "Retaliatory Deterrence in Cyberspace." *Strategic Studies Quarterly* (Air University Press), no. Spring (2011): 62-80.

Story, Kurt S. "Protecting SPACE in a Contested and Congested Domain." *Army Space Journal* (US Army Space and Missile Defense Command) 9, no. 1 (2010): 8-9, 15.

Theohary, Catherine A. and John Rollins. *Terrorist Use of the Internet: Information Operations in Cyberspace.* CRS Report for Congress, Washington D.C.: Congressional Research Service, 8 March 2011.

"Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space Including the Moon and Other Celestial Bodies ." *Island One Society.* 1967. http://www.islandone.org/Treaties/BH500.html (accessed December 11, 2011).

Vermeer, Arjen. "The Laws of War in Outer Space: Some Legal Implications for the Jus ad Bellum and the Jus in Bello of the Militarisation and Weaponisation of Outer Space." *Inter-Disciplinary.Net.* http://www.inter-disciplinary.net/ptb/wvw/wvw4/Vermeer%20paper.pdf (accessed December 9, 2011).

West, Jessica. "Back to the Future: The Outer Space Treaty turns 40." *The Ploughshares Monitor* 28, no. 3 (2007).

Wicker, Christian. *The Concepts of Proportionality and State Crimes in International Law.* Frankfurt am Main: Peter Lang GmbH, 2006.

# Notes

[1] Douhet, p. 80. Full quote: *"'Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur. In this period of rapid transition from one form to another, those who daringly take to the new road will enjoy the incalculable advantages of the new means of war over the old. This new character of war, emphasizing the advantages of the offensive, will surely make for swift, crushing decisions on the battlefield. Those nations who are caught unprepared for the coming war will find, when war breaks out, not only that it is too late for them to get ready for it, but that they cannot even get the drift of it. Those who are ready first not only will win quickly, but will win with the fewest sacrifices and the minimum expenditure of means."*

[2] Qiao, p. 47

[3] Coleman

[4] Story, p. 9

[5] Coleman

[6] Ibid.

[7] Ryan

[8] Chinese Anti-Satellite (ASAT) Capabilities

[9] *Cyberpower and National Security*, pp. 177-8, 418

[10] Goodin

[11] Markoff

[12] Farwell, pp. 23-4, 31

[13] Cheng, p. 4

[14] Morgan, F., p. 16

[15] *International Strategy for Cyberspace*, pp. 3-4

[16] *National Space Policy of the United States of America*, p. 1

[17] *Charter of the United Nations*, pp. 10-11

[18] *International Strategy for Cyberspace*, p. 10

[19] *National Space Policy of the United States of America*, p. 3

[20] *International Strategy for Cyberspace*, p. 13

[21] *National Space Policy of the United States of America*, p. 14

[22] *Cyberpower and National Security*, p. 335

[23] Harknett, p. 9

[24] Sterner, p. 69

[25] Chilton & Weaver, p. 32

[26] Morgan, F., p. xii

[27] Harknett, p. 9

[28] Harknett, p. 9

[29] Ibid.

[30] Beidleman, p. 15-6

[31] Libicki, p. 179

[32] Farwell, p. 30

[33] *Cyberpower and National Security*, p. 527

[34] Ibid, pp. 527-8

[35] Ibid, p. 528

[36] Ibid, p. 528

[37] Ibid, pp. 528-9

[38] Ibid, p. 529

[39] Ibid, pp. 529-30
[40] Ibid, pp. 530-1
[41] Libicki, p. 84
[42] Using Schmidt's framework, the table below provides an analysis on whether some historical incidents would be considered an armed attack and met the threshold authorizing a forceful response.

| Act | Legitimate Act? | Use of Force Armed Attack? | Forceful Response Authorized? |
|---|---|---|---|
| Hackers Attack on British MOD Satellite | No. Not a legitimate/legal act | No. No damage done. Did not meet a minimum threshold | No. Britain would not be authorized to retaliate by force |
| Hackers taking control of US owned NASA satellites | No. Not a legitimate/legal act | No. No damage done. Did not meet a minimum threshold. | No. US would not be authorized to retaliate by force |
| Chinese ASAT | No, if used against a non-Chinese system in a peacetime setting. In this case, it was legitimate as it was against own system, but China failed to take into account collateral damage possibilities. | Yes. An ASAT attack would cross a threshold of an armed attack | Unlikely for a single satellite. No human casualties and burden of proof on attacked nation to justify level of economic, social and political damage to authorize a forceful response. |
| Estonia Cyberattack | No. Not a legitimate/legal act | Yes. Due to its immediacy, directness, invasiveness and measurability, this attack qualifies as use of force. | Unlikely, as no human casualties sustained and the effects of the attack were not permanent and attribution not established. |
| Georgia Cyberattack | Yes, as it was in concert with on-going conflict. Whether the conflict was legal is not under consideration. | Yes. Due to its immediacy, directness, invasiveness and measurability, this attack qualifies as use of force. | Yes, as it occurred during active conflict. Active conflict would reduce burden of proof on legitimacy. |
| Stuxnet Worm | No. Not a legitimate/legal act | Yes. Due to its design and destruction of real property, likely qualifies as a use of force. | No. Level of impact not high enough to authorize a forceful response. |

[43] Harknett, p. 10
[44] Laasme, p. 59
[45] Ryan.
[46] Carr, *Stuxnet's Finnish-Chinese Connection*. In his article, Mr. Carr examines other theories on the source of the Stuxnet worm, including that it originated in China as a way to covertly deny Iran its nuclear program while preserving relations with Iran, a major supplier of oil to China
[47] Harknett, p. 10
[48] Morgan, F., p. 15
[49] McMillian, "Iran was Prime Target of SCADA Worm." In his article, Mr. McMillian describes how Stuxnet exploits a vulnerability in the Windows OS and requires human interaction to spread via a USB device.
[50] Sterner, p. 66
[51] Theohary, p. 6
[52] Harknett, p. 10
[53] *Charter of the United Nations*, pp. 10-11
[54] Wicker, p. 61
[55] Reagan
[56] McIntyre
[57] Wicker, p. 64
[58] The "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies" is commonly referred to as the "Outer Space Treaty"
[59] Vermeer, p. 1
[60] Article IX of the Outer Space Treaty states: States Parties to the Treaty shall pursue studies of outer space, including the Moon and other celestial bodies, and conduct exploration of them so as to avoid their harmful contamination and also adverse changes in the environment of the Earth resulting from the introduction of extraterrestrial matter and, where necessary, shall adopt appropriate measures for this purpose. If a State Party to the

Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State Party to the Treaty which has reason to believe that an activity or experiment planned by another State Party in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, may request consultation concerning the activity or experiment. (85p13)

[61] Johnson-Freese

[62] West, p. 4

[63] Chilton & Weaver, p. 40

[64] Libicki, p. 179

[65] Chilton & Weaver, p. 39-40

[66] *Cyberpower and National Security*, p. 16

[67] Wicker, pp. 38-9

[68] Ibid, p. 40

[69] Morgan, Forrest, p. 17

[70] Wicker, pp. 46-7

[71] Sterner, p. 72

[72] Sterner, p. 72

[73] Pavlischek, p. 21

[74] Chilton & Weaver, p. 40

[75] According to Holger Stark in SpielelOnline, over 100,000 systems worldwide have been infected by the Stuxnet worm. Mr. Jeffrey Carr published two articles that suggest the possibility that the Stuxnet worm may have contributed to an unplanned outage at a British nuclear power plant and the loss of India's INSAT-4B satellite. While no corroborating data was found, the ambiguity of the failures and Mr. Carr's arguments present an interesting case.

[76] Chilton & Weaver, p. 39

[77] Chilton & Weaver, p. 34

[78] Morgan, F., p. 31

[79] Chilton & Weaver, p. 40

[80] Libicki, p. 83-4

[81] Ibid., p. 84

[82] Morgan, F., p. xiii

[83] Sterner, p. 72

[84] Ibid.

[85] Laasme, p. 60

[86] Chilton & Weaver, p. 39

[87] Ibid.

[88] Ibid.

[89] Morgan, F., p. 43

[90] Chilton & Weaver, p. 39

[91] *National Space Policy of the United States of America*, p. 7

[92] Harknett, p. 7

[93] *National Security Strategy of the United States*, p. 12

[94] Sterner, pp. 71-2

[95] *National Security Strategy of the United States*, p. 22

[96] Sterner, pp. 71-2
[97] Morgan, F., pp. 44-5
[98] Chilton & Weaver, p. 38
[99] Story, p. 15
[100] Harknett, pp. 8-9