SPACE & DEFENSE

Volume Eight Number One SPRING 2015

EISENHOWER CENTER
FOR SPACE AND DEFENSE STUDIES

Space & Defense

Journal of the United States Air Force Academy
Eisenhower Center for Space and Defense Studies

Space & Defense is available at http://www.usafa.edu/df/dfe/dfer/centers/ecsds/defense_journal.cfm and indexed by ©EBSCO*host*.

Editor, *Space & Defense*
Dept. of Political Science
2354 Fairchild Dr., Suite 6L-116
USAF Academy, CO 80840

Space & Defense

Journal of the United States Air Force Academy
Eisenhower Center for Space and Defense Studies

Volume Eight ▪ Number One ▪ Spring 2015

Editor's Note

S&D recruits more international contributors and opens its aperture to welcome articles on the political economy of space.

This issue of the journal begins our editorial push to feature more peer-reviewed contributions from international authors. Last summer, I had the opportunity to attend the ISA-FLACSO joint meeting in Buenos Aires, Argentina. The exchange brought together members of the largest international studies association in the United States with social sciences faculty from prestigious universities in Latin America. Not only did this journal receive two papers from the meeting (on cyber war from Brazil and on developing launcher programs from Argentina), it also became clear that implications of the "3 C's" for space—the domain becoming more congested, competitive, and contested—reach well beyond arms control and traditional international security of the great powers.

Rapidly growing political consensus that American leadership in the world faces enormous challenges after large-scale military disappointments in Iraq and Afghanistan along with ongoing fiscal crises at home is bound to push national security and questions of political economy, after a long hiatus, back together. A recent chairman of the U.S. Joint Chiefs of Staff identified spiraling national debt as the most dangerous threat to the United States, and his successor, General Martin Dempsey, last year articulated the most pressing challenge for the military as adapting operations, "the bend of power," in order to make do with less—i.e., fewer personnel and scarcer dollars for technology modernization—while doing just as well.

Of course, one of the few ways to do more with less, if this is even possible at the grand strategic level, is to pull from some other shelf, or draw from another resource that has fallen into disuse. The wherewithal to bend steel, to reorganize a restricted defense budget in order to produce a more effective military under changing international conditions, has to come from somewhere, and a natural field to explore, given previous interaction with International Security, is Political Economy.

As U.S. military presence and actions in the world subside how do international flows in trade, investment, and information bear upon national development policies? Where are the points of contact within transnational, regional, national, or subnational institutions at which smart, low-intensity or nonviolent military intervention could make a difference? During the Cold War, political economy was addressed, problematically, by cultivating militarized methods for eliminating recalcitrant factions or toppling rogue regimes in the Third World. One difference between then and now is the United States does not face implacable ideological adversaries backed by economic and military resources of a superpower patron, so there may be more room for cooperation with incumbent governments, the sort of relationship that could lead to mutual learning on critical security issues rather than naked subordination to priorities of American national defense.

According to the most recent Quadrennial Defense Review (2014), and with the same sentiment permeating the 2015 National Security Strategy and national space policy documents, the United States needs new and renewed partnerships, now. Presumably, the ailing unipole needs them more than it did during troubled times of the late Cold War when Kenneth Waltz wrote about stability of bipolarity and superpower status against allied defections or flirtations like, in those days, West German *Ostpolitik.* At the same time, potential interlocutors, today, have less need for the United States.

In the wake of the ISA-FLACSO conference, Brazilian diplomacy, including relevant aspects of space policy, is a case in point. On major international questions—Western agricultural subsidies haunting the Doha Round of world trade talks; nuclear sanctions on Iran; lease agreements with foreign tech giants to exploit massive

petroleum reserves in the *pre-sál* layer off the coast of São Paulo; sanctioning Russia for military aggression against Ukraine; or supporting Israeli reprisals against Hamas militants in Gaza, Brazil's voice has cut across U.S. policy, making it harder for the United States to attain strategic goals. Added to the crowded field calling America's global leadership into question, Brazil's demonstrated independence complicates scholars' notions—scholars ranging from John Mearsheimer to Barry Buzan—of U.S. *regional* hegemony. Brazil, it turns out, is relatively free to drive a hard bargain, to partner with the United States or compete against "the last remaining superpower," as Brazil's interests demand.

The same sort of mixed-motive game is playing out in space. Space policy both reflects the global dynamic of a struggling hegemon and helps shape it. While the United States holds a technological lead, Brazil is eager to cooperate, and there has been significant cooperation from the training of a Brazilian astronaut to design of satellite platforms for oceanographic observation. Yet, the Brazilian pioneer in question ended up flying to low-earth orbit on a Russian ship, and with respect to a parallel attempt to develop indigenous launch capability, Brazil forged agreements with U.S. competitors such as China and Ukraine.

The advent of competitive and congested space places U.S. defense institutions in a dilemma unlike those they faced for much of the Cold War. They must continue to guard a precious technological advantage from potential rivals, but now they are obliged to huckster as well. Increasingly, many would-be partners have attractive alternative options. One technical manager in Latin America described a trend for space operations that captures a conundrum for the United States, generally. Emerging space nations want to work with the United States because of the financial capital and state-of-the-art technology the incumbent leader in space brings to the table, but when it comes to institutional cooperation, the United States decides which technologies are dual-use. In order to prevent diffusion and erosion of its military advantage in space technology, the United States imposes restrictions on personnel and parts that are permitted in joint projects, causing unexpected delays and extra production costs.

Junior partners tolerate these while U.S. equipment and know-how reigns supreme, but the technology gap with other suppliers such as Europe, China, Russia, and Brazil is closing. If Brazil, for example, can fulfill a simpler and more efficient cooperation agreement to assist a smaller economy with modern earth observation satellites, Brazilian companies may capture business, developing with junior partners their own market niche that excludes the United States. If the United States does not share more, its lead will deteriorate in commercial space technology; yet, if it does sweeten offers of cooperation with new partners by lowering restrictions, its military advantage could disappear.

The United States cannot resolve its grand strategic dilemma by declaring simply that it will play the benign hegemon, providing global goods, including space knowledge and services for national development, at the same time it retards other states by starving them of dual-use technology. The window for a strategy of uncompromising space dominance is closing along with America's technological margin. In order to extend its influence, and thereby secure its defense, the United States will have to share more and exclude less to retain the best international partners. Finding the right balance between enlightened service to the global system and classic controls for national security will demand tailored negotiations, based upon extensive knowledge of *comparative* political economy. This is "actor-specific" knowledge that Alexander George famously touted in *Bridging the Gap* (1993), and it reflects an antecedent intellectual movement when International Political Economy merged with comparative politics to better identify favorable conditions, applicable to various states in different regions of the world, for development and successful integration into the global system.

Observing the discussion at ISA-FLACSO and speaking with experts on the sidelines of the meeting, it was clear that foreign policy in Latin America remains attuned to ideas percolating at the intersection of International Security, IPE, and

Comparative Politics. The theme of the meeting was "Global and Regional Powers in a Changing World," and several speakers anticipated historic shifts in the international distribution of power not from class warfare or revolution in leading states but from diffusion of technology and asymmetric gains in labor productivity for rising powers.

A changing of the guard for international political economy was thought to create a raft of new opportunities for midsize economies like Argentina's and those even smaller. Information-age industries did not require huge military complexes or enormous capital reserves but smart investments by governments in education and communications in order to attract foreign capital and boost the private sector. Excitement over emerging technologies and historic shifts on the horizon for global order moved discourse to the right. There was less talk about resisting hegemonic exploitation and more on how to prepare states in the wings of global competition to thrive during the fresh economic and political challenges to come, encompassing planetary not just national defense.

In contrast to the buzz surrounding high technology, there was surprisingly little talk about roles civil or commercial space might play in upcoming global and regional power shifts. This silence belied the growth in long-distance telecommunications and demand for terrestrial information derived from space imagery. It also introduced the United States, seeking to strengthen national defense through new partnerships and deepening cooperation, to a new variant of a familiar strategic puzzle. The solution on how to approach developing space nations, even as the domain becomes more "congested, competitive, and contested," will require actor-specific information as well as grand strategic thinking.

Argentina and Brazil, for example, relative to the United States occupy roughly similar structural positions in the international political economy of space activity. Brazil may spend five to ten times more money than Argentina on space, but both Latin American powers spend less than one percent of the U.S. budget. Nevertheless, in spite of their similar positions and parallel ambitions to build a complete national program—adding launch and design to satellite operation capacity—Brazil and Argentina manage their national efforts with respect to civil-military relations very differently. Lacking actor-specific information contextualized within a broad strategic framework, the United States risks unnecessary blunders, aggravating political sensitivities and ruining investments, as it competes with Russia and China to win the business and forge cooperative networks with emerging space actors.

This journal, *Space & Defense*, and its host, the Eisenhower Center at the United States Air Force Academy, can contribute to policy by promoting and disseminating systematic research, both theoretical and empirical, on the new political economy of space services. Decision makers might then draw upon the best possible expert knowledge when negotiating—with a diverse range of partners—accords at once mutually beneficial and consistent with United States defense strategy in a changing world. As a uniquely powerful state within the global system, the United States, while continuing to counter adversaries and reassure allies, supports a progressive international order that reflects its own Constitutional principles, facilitates productive compromises, and, frankly, reduces the costs of wielding influence. In the daily rush of events, national security and foreign policy bureaucracies are hard-pressed to study either general principles or critical idiosyncrasies of emerging space powers. Whenever ethical policy making and social science method combine, *Space & Defense* would like to nurture practical knowledge of political economy at the nexus of government, industry, and academia.

Damon Coletta
USAFA
`
April 2015

Strategic Nuclear Weapons for Planetary Defense

James Howe

A Global-Zero world, one without nuclear weapons, might leave the planet more vulnerable.

The planet Earth is continually under bombardment.[1] Each day, roughly 100 tons of small meteoroids and space debris – some as large as a meter in diameter, but most smaller than a grain of sand – strike the atmosphere.[2] Moving at speeds in excess of 40,000 kilometers per hour, these meteoroids are often seen as bright streaks in the sky as they burn up from atmospheric friction.[3] Fortunately, because they are consumed high in the atmosphere, meteoroids and space dust pose no threat to humans or other life on Earth.

Unfortunately, there are larger objects in orbit around the Sun that can pose a significant threat to the planet. It is estimated that as many as a billion asteroids and possibly two trillion comets inhabit the solar system.[4] Asteroids range in size from a meter to hundreds of kilometers in diameter: the solid nuclei of comets can be several kilometers wide. For both asteroids and comets, the larger their size, the less frequently they appear in nature. While the vast majority of asteroids orbit between Mars and Jupiter, a very small percentage of them are on elliptical paths that cross Earth's orbital track, along with a much smaller number of comets. Of these, some invariably collide with our planet.[5]

On average, an asteroid between 30-50 meters in size strikes Earth every 100-200 years.[6] Such asteroids are capable of inflicting damage over a wide area and have the potential for killing thousands of people. Much larger asteroids, although exceptionally rare, can inflict catastrophic damage: an asteroid ten kilometers wide struck Earth 65 million years ago and extinguished most life on the planet, including all species of dinosaurs.[7]

In recent decades scientific understanding of the asteroid and comet population has grown, prompting efforts to protect the planet from a devastating collision. Known as 'planetary defense,' these efforts encompass locating and tracking threatening bodies as well as developing means for mitigating a potential impact. The general concept is to identify a threatening space object many years in advance and then deflect it, by changing its velocity, or fragment it into smaller pieces. Theoretically, mitigating potential impacts of small and mid-sized bodies – those up to 1000 meters in diameter – could be accomplished using non-explosive means, although the largest asteroids or those detected shortly before impact might only be deflected or fragmented using the explosive power of nuclear weapons.

---

[1] James Howe served for twenty-seven years on active duty in the U.S. Coast Guard and has earned master's degrees from the U.S. Marine Corps War College, Harvard University (Extension School), and the American Military University.

[2] National Research Council, *Defending Planet Earth: Near-Earth-Object Surveys and Hazard Mitigation Strategies* (Washington, D.C.: the National Academies Press, 2010), 12.

[3] John S. Lewis, *Rain of Fire and Ice: The Very Real Threat of Comet and Asteroid Bombardment* (Lexington, KY: Perseus Publishing, 1996), 37.

[4] David J. Eicher, *Comets! Visitors from Deep Space* (New York: Cambridge University Press, 2013), 8.

[5] Clark Chapman and Ed Lu, "FAQ on the Chelyabinsk Meteor Impact," B612 Foundation, February 18, 2013, accessed June 21, 2014, https://b612foundation.org/news/faq-on-the-chelyabinsk-asteroid-impact/.

[6] National Aeronautics and Space Administration, *Near-Earth Object Survey and Deflection Analysis of Alternatives*, Report to Congress, March 2007, 6.

[7] Walter Alvarez, *T. Rex and the Crater of Doom* (New York: Vintage Books, 1997), 3-6.

ASSESSING THE THREAT

Each asteroid and comet is unique in its composition, shape, size, and orbit. While most small asteroids are solid masses, many larger asteroids are a collection of smaller bodies held together by a weak gravitational bond, akin to an orbiting pile of rubble. Other asteroids are known as binaries, with two bodies gravitationally associated with one another.[8] Typically, asteroids are composed of iron, carbon, or silica. Conversely, the nuclei of comets consist of frozen gases and dust. As they approach the Sun, the gases in the comet's nucleus evaporate and create the signature tail that often can be observed from Earth. Some comets have exhausted the store of frozen gases in their core and consist primarily of asteroid-like materials; from a distance it often is impossible to distinguish between these extinct comets and true asteroids.[9]

Asteroids originated from the failed formation of a rocky planet billions of years ago. Fragments of the planet remained in orbit around the Sun and, over the eons, suffered millions of collisions, breaking into smaller pieces. Most asteroids orbit the Sun once each 4-5 years and many have had their orbit changed through collision or, more likely, by the gravitational influence of Jupiter and other bodies.[10] Alternatively, comets originate from deeper in space. Most short-period comets emanate from the Kuiper Belt, located beyond Neptune, and have an orbital period of up to 200 years, while long-period comets hail from the Oort Cloud, a band of debris at the furthest reaches of the solar system, and can take between 200 and several thousand years to conduct one revolution around the Sun.[11]

Of the small percentage of asteroids that do not orbit in the main asteroid belt, scientists have discovered more than 12,000 that will pass within 1.3 Astronomical Units, or 200 million kilometers of the Sun.[12] These have been dubbed 'Near Earth Asteroids' and together with a much smaller population of comets are categorized as 'Near Earth Objects' (NEO).[13] Based on a variety of orbital characteristics, most NEOs pose no threat as they will never intersect Earth's track through space; only about one-fifth of NEOs will approach within 0.05 Astronomical Units (eight million kilometers) of Earth's orbit. These asteroids and comets are classified as 'Potentially Hazardous Objects' (PHO) and are the focus of planetary defense detection, tracking, and mitigation planning efforts.[14]

The kinetic energy imparted to Earth from an asteroid or comet collision is determined by the mass and relative velocity of the impacting body. Because mass cannot be known with certainty for most asteroids or comets, rough estimates of potential damage are based on the physical size of the object. Smaller asteroids, between one and 30 meters in diameter, typically do not have sufficient mass to complete the journey through Earth's atmosphere and burn up, disintegrate, or explode before reaching the planet's surface. Such asteroid explosions are known as 'bolides' and typically create a large fireball. The shock wave from an aerial explosion is often large enough to cause damage on the ground, as seen in February 2013, when an asteroid estimated at 15-20 meters in diameter exploded over Chelyabinsk, Russia, injuring more than 1000 people.[15] Detection of these small asteroids is extremely difficult and less than 0.01 percent have been located; because they pose a limited threat, planetary defense efforts typically do not focus on

[8] Roger Dymock, *Asteroids and Dwarf Planets* (New York: Springer, 2010), 33-35.
[9] Lewis, 42-43.
[10] Martin Rees, ed., *Universe: The Definitive Visual Guide* (New York: DK Books, 2005), 170-172.
[11] Eicher, 9.
[12] National Aeronautics and Space Administration, "Near Earth Object Program," National Aeronautics and Space Administration, March 22, 2015, accessed March 22, 2015, http://neo.jpl.nasa.gov/stats/.
[13] William Ailor, "Planetary Defense Conferences: Sharing Information on NEO Threats and Mitigation" (paper presented at the meeting of the Working Group on Near Earth Objects of the Scientific and Technical Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space, Vienna, February 2011), 4.
[14] Lindley Johnson, "Near Earth Object Observations Program" (paper presented to the Planetary Defense Task Force, Cambridge, MA, April 15, 2010), 3.
[15] Chapman and Lu.

asteroids below 30 meters in diameter.[16]
It is the larger asteroids and comets that concern planetary defense practitioners, particularly the objects of intermediate size that have not yet been located, but could produce significant damage to Earth. A prime example is the asteroid or comet that exploded over Tunguska, Russia in June 1908. This celestial body, estimated at 40 meters in diameter, disintegrated and exploded over a heavily wooded area, creating a tremendous shock wave that flattened 2000 square kilometers of forest, as shown in Figure 1 – a blast nearly 200 times more powerful than those of the nuclear bombs used in World War II.[17] Had the Tunguska object exploded over a populated area hundreds if not thousands of lives could have been lost.

Asteroids between 30-100 meters in diameter are known colloquially as 'city killers' and could devastate a small region on Earth, as vividly demonstrated in Tunguska. Larger 100-300 meter 'nation killer,' 300-1000 meter 'continent killer,' and 1000-plus meter 'civilization killer' objects would inflict proportionally more damage: a massive crater created by the impact of a five-kilometer wide asteroid is depicted in Figure 2. The even larger asteroid that struck near the Yucatan Peninsula 65 million years ago – one of several known mass extinction events in the history of Earth – generated a global cataclysm of tsunamis, earthquakes, and fire. The thick shroud of smoke and debris created by the collision encircled the globe for hundreds of years and snuffed out nearly three-quarters of all living species on the planet.[18]

Many of the more than 12,000 NEOs detected so far are large asteroids. Ongoing surveys of outer space have located roughly 95 percent of the estimated population of 900 civilization-threatening asteroids that pass near Earth's orbit. As the size of threatening asteroids decreases, however, the percentage of those that have been detected also decreases. Of the 4800 continent killer PHOs estimated to be in existence, roughly half have been found, and only ten percent of nation killers have been located. As for the smaller yet still dangerous city killers, of which 500,000 are believed to exist, only one percent have been identified.[19] While thousands of comets have been discovered, the much longer period of their orbits creates a great deal of uncertainty as to how many may pose a hazard to the planet.[20]

There is roughly a 50-50 probability that a city killer asteroid will strike Earth during an average human lifespan, and a much lower probability for an impact by a larger space object. While the mean time between collisions from city killer asteroids is one or two centuries, the time between collisions with larger asteroids is measured in millennia, or even millions of years for those that can threaten mass extinction.[21] Nonetheless, the data available to forecast future threats is extremely limited and there is no way to ascertain with any degree of precision when the next major asteroid or comet collision will occur. There is no scientific doubt that Earth will face the hazard of a devastating asteroid or comet impact at some unknown point in the future.

COLLISION MITIGATION TECHNIQUES

A number of different methods have been posited for preventing an asteroid or comet from colliding with Earth. These proposed methods could be employed independently or in tandem.

---

[16] Benjamin Deniston, "2013 Planetary Defense Conference: Rising to the Challenge," *21st Century Science & Technology* (Summer 2013): 29.
[17] National Aeronautics and Space Administration, "The Tunguska Impact – 100 Years Later," NASA Science, June 30, 2008, accessed February 18, 2014, http://science.nasa.gov/science-news/science-at-nasa/2008/30jun_tunguska/.
[18] Lynn Yaris, "Alvarez Theory on Dinosaur Die-Out Upheld: Experts Find Asteroid Guilty of Killing the Dinosaurs," Berkeley Lab, Lawrence Livermore National Laboratory, U.S. Department of Energy, March 9, 2010, accessed June 25, 2014, http://newscenter.lbl.gov/feature-stories/2010/03/09/alvarez-theory-on-dinosaur/ and John Kunich, "Planetary Defense: the Legality of Global Survival," *Air Force Law Review 41* (1997): 121.
[19] Deniston.
[20] Hans Rickman, "Current Questions in Cometary Dynamics," in *Comets II*, ed. M.C. Festou, H.U. Keller, and H.A. Weaver (Tucson: the University of Arizona Press, 2004), 205-206.
[21] National Research Council, 19.

Three key variables will help guide the selection of the appropriate response to a predicted strike: the time until impact and the size and composition of the asteroid or comet. Other factors such as the amount of spin or the shape of the asteroid may also drive the mitigation strategy.[22]

Potential mitigation techniques using existing technology – or technology that can be modified for planetary defense in a short time span – can be placed into three general categories: 'slow push' methods, kinetic impacts, and nuclear strikes. Most of these methods are designed to deflect the asteroid by changing its velocity so that it passes Earth harmlessly. The earlier a deflection can be undertaken, the less total change in velocity will be necessary. For interventions more than a decade in advance of the collision, a change of only about one centimeter per second typically is sufficient.[23] In addition to deflection techniques, another mitigation method is to fragment the object, so that no large pieces remain to strike the planet.[24]

The 'slow push' methods span a variety of techniques that could, in theory, deflect most city and nation killer asteroids, both solid and porous, provided the threat was detected one or more decades in advance. Lasers or concentrated solar rays could be beamed onto the asteroid, causing surface material to burn off while generating a small counterforce; one concept would employ a series of large Earth-orbiting satellites to harness sunlight for this purpose.[25] A second method would employ robotic spacecraft to hover close to the asteroid so that the slight gravitational attraction between the two bodies would, over several years, alter the asteroid's velocity. Other proposed methods would attach rocket motors to the surface of the asteroid, modify the albedo of a rotating asteroid to change the amount of photon re-radiation, or mine the asteroid's surface, ejecting materials at high speed – all to produce a slight cumulative change in the velocity of the threatening body.[26]

Kinetic impacts would involve flying a spacecraft into the asteroid to impart, through the collision, sufficient kinetic energy to alter the asteroid's velocity. Technologically, this is the simplest mitigation technique and is likely to be the preferred option for protecting against smaller threatening bodies, or in cases where multiple decades are available to deflect asteroids up to 1000 meters in diameter.[27] Depending on the size of the asteroid and the time before impact, however, a number of kinetic strikes might be necessary. Kinetic strikes would be most effective against solid objects but far less useful for altering the velocity of porous bodies or 'rubble pile' asteroids.[28] Kinetic strikes designed to eject a maximum amount of surface material from the asteroid or comet into space would most effectively change its velocity.[29]

Nuclear strikes may be the only available option for mitigating the threat of a larger asteroid or where there is little time between initial detection and the expected collision with Earth.[30] Explosive

[22] Bong Wie, "Hypervelocity Nuclear Interceptors for Asteroid Deflection or Disruption" (paper presented at the 2011 IAA Planetary Defense Conference, Bucharest, Romania, May 9-12, 2011), 2.
[23] Keith A. Holsapple, "About deflecting asteroids and comets," in *Mitigation of Hazardous Comets and Asteroids*, ed. M.J.S. Belton, T.H. Morgan, N. Samarasinda, and D.K. Yeomans (New York: Cambridge University Press, 2004), 114.
[24] R.B. Adams et al, *Survey of Technologies Relevant to Defense from Near-Earth Objects*, NASA/TP-2004-213089 (Huntsville, AL: National Aeronautics and Space Administration, 2004), 62-65.
[25] University of California Santa Barbara, "News Release: California Scientists Propose System to Vaporize Asteroids That Threaten Earth," University of California, February 14, 2013, accessed March 30, 2014, http://www.ia.ucsb.edu/pa/display.aspx?pkey=2943.
[26] National Aeronautics and Space Administration, *Near-Earth Object Survey and Deflection Analysis of Alternatives*, 20.
[27] Jesse D. Koenig and Christopher F. Chyba, "Impact Deflection of Potentially Hazardous Asteroids Using Current Launch Vehicles," *Science and Global Security* 15 (2007): 67.
[28] Christian Gritzner and Ralph Kahle, "Mitigation technologies and their requirements," in *Mitigation of Hazardous Comets and Asteroids*, ed. M.J.S. Belton, T.H. Morgan, N. Samarasinda, and D.K. Yeomans (New York: Cambridge University Press, 2004), 177.
[29] National Research Council, 73-74.
[30] Wei, 1.

force from a nuclear weapon could create, in an instant, sufficient kinetic energy to alter the velocity of all but the largest asteroids. The immense power of a nuclear device detonated on, near, or under the surface of a threatening space object could deliver several orders of magnitude more force, in one instant, than the kinetic impact or slow push techniques.[31] Alternatively, a nuclear explosion could be used to break the asteroid into thousands of pieces, so that only a small percentage of the object's mass would strike the atmosphere.

The explosive yield of a nuclear weapon is vastly greater than that of an equivalent size of conventional, chemical explosive, such as the commonly used trinitrotoluene (TNT). The first nuclear weapon – a plutonium fission device exploded during the Trinity test in July 1945 – had an explosive yield estimated at 20,000 tons (20 kilotons) of TNT. Seven years later, the first thermonuclear fusion bomb was tested and yielded 10,400,000 tons (10.4 megatons) of explosive energy. The largest nuclear weapon ever demonstrated was a Soviet device exploded in October 1961. Dubbed *Tsar Bomba*, it produced more than 50 megatons of energy. Small, battlefield tactical nuclear weapons were fielded by both the U.S. and the USSR, with yields often in the single kilotons; modern fission devices tested by India, Pakistan, and North Korea produced yields in a similar range.[32]

There is an ample stockpile of nuclear devices potentially suitable for a planetary defense mission. The United States currently possesses around 7100 nuclear weapons, 2080 of which are strategically deployed and the remainder of which are in storage, reserve, or awaiting dismantlement. U.S. nuclear weapons are designed as bombs, to be dropped on target by aircraft, or warheads, to be launched aboard land-based or submarine-based ballistic missiles. While larger weapons were developed, currently the maximum yield in the U.S. arsenal is around one megaton, with most weapons designed to yield 100-500 kilotons.[33] Russia has a similar number of nuclear weapons, with about 1640 deployed, several thousand in reserve or awaiting dismantlement, and 2000 with tactical yields. Other major nuclear powers include France, with less than 300 operational weapons; China, with about 240 warheads; Great Britain, with a total stockpile of around 225; and India, Israel, and Pakistan, each with roughly 100 devices.[34]

EMPLOYING NUCLEAR WEAPONS

The general concept for a planetary defense mission using a nuclear weapon would be to launch a warhead aboard a rocket capable of interplanetary travel, to intercept the threatening body at the optimal spot in its orbit in order to maximize the effectiveness of the deflection or fragmentation. The nuclear device could be detonated in one of three configurations: as a stand-off blast above the surface, on the surface, or beneath the surface of the asteroid or comet.[35] One concept for a nuclear explosive asteroid interceptor is shown in Figure 3.

A stand-off blast could be used for deflection, as it would provide a massive force to alter the object's trajectory while minimizing the possibility of fracturing. In comparison to surface or sub-surface blasts, a stand-off detonation would require a less sophisticated intercept maneuver and could be accomplished using a simpler delivery system. The nuclear device would be maneuvered close to the asteroid, notionally to a height equal to 25 percent of the asteroid's radius and above a specific hemisphere of the asteroid to

[31] National Aeronautics and Space Administration, *Near-Earth Object Survey and Deflection Analysis of Alternatives*, 21-24.
[32] Comprehensive Test Ban Treaty Organization, "Types of Nuclear Weapons," Comprehensive Test Ban Treaty Organization, January 2012, accessed April 7, 2014, http://www.ctbto.org/nuclear-testing/types-of-nuclear-weapons/.
[33] Hans M. Kristensen and Robert S. Norris, "US nuclear forces, 2015," Bulletin of the Atomic Scientists, March 3, 2015, accessed March 21, 2015, http://thebulletin.org/2015/march/us-nuclear-forces-20158075.
[34] Daryl Kimball, "Nuclear Weapons: Who Has What at a Glance," Arms Control Association, February 2015, accessed March 22, 2015, http://www.armscontrol.org/factsheets/nuclearweaponswhohaswhat.
[35] Holsapple, 123-125.

enhance the deflective force.[36] Upon detonation, the thermal impulse and nuclear radiation generated in the explosion would be absorbed by surface materials, which would instantly heat up or vaporize.[37] This would peel off a layer of rock and eject it into space, imparting a reactive force to alter the asteroid's velocity. Computer modeling has shown that a typical stand-off blast could ablate about one percent of an asteroid's total mass.[38] The higher above the surface the nuclear weapon was detonated, the thinner and wider would be the layer ejected.[39]

In most cases the preferred direction of the velocity change would be along or directly opposite the asteroid's orbital path, in order to change the period of the object's revolution around the Sun and avoid the forecast collision with Earth.[40] This concept of speeding up or slowing down the threatening body, rather than pushing it sideways, applies to all long-lead-time deflection techniques including slow push and kinetic impact methods. However, for deflection missions that occur close to the time of collision with Earth – notionally when the asteroid is on its terminal orbit before impact – a sideways deflection using a large explosive force could be the most effective mitigation strategy.[41]

Surface and sub-surface blasts could be used either for deflection or fragmentation. The most efficient transfer of energy from a nuclear weapon to an asteroid would occur when the device was exploded beneath the surface of the object; in comparison to a stand-off blast a sub-surface detonation would transfer up to 100 times more energy.[42] However, surface or sub-surface blasts would increase the possibility that a planned deflection would instead fragment the asteroid. To avoid this possibility, time permitting, an exploratory mission to the threatening asteroid or comet could ascertain its material composition and internal structure, and the most effective mitigation strategy could be devised with that data.[43]

A surface or sub-surface blast would create a large crater and eject a mass of debris into space. The deeper the sub-surface device was located, the more effectively energy would be imparted to the asteroid. This is important for fragmentation missions where the threatening body would be blasted into thousands of smaller pieces. One analysis found that for fragmentations conducted three or more years ahead of a projected impact, more than 99.999 percent of an asteroid's original mass would miss Earth completely.[44]

A difficult challenge for carrying out a sub-surface burst involves placement of the nuclear device, particularly in circumstances with short-lead time where the device must be transported directly to the asteroid at high velocity. To assure effectiveness in fragmentation or deflection, the nuclear weapon must strike the asteroid at a precise impact angle and penetrate to the proper depth. Unfortunately, a high velocity impact is likely to vaporize the nuclear device upon contact. To allow the nuclear warhead to burrow to the proper depth, a two-segment penetrator configuration could be employed. As originally conceived by Russian researchers and refined at the Asteroid Deflection Research Center at Iowa State University, a hypervelocity nuclear interceptor could be comprised of a dual-bodied spacecraft, with the forward section serving as a kinetic impactor and the aft section containing the nuclear weapon. Upon impact, the kinetic device would blast open a narrow crater in which the

[36] Ibid., 117.
[37] Donald B. Gennery, "Deflecting Asteroids by Means of Standoff Nuclear Explosions" (paper presented at the 2004 Planetary Defense Conference, Orange County, CA, February 23-26, 2004), 1.
[38] D.S. Dearborn, S. Patenaude, and R.A. Managan, "The Use of Nuclear Explosives to Disrupt or Divert Asteroids" (paper presented at the Planetary Defense Conference, Washington, DC, March 5-8, 2007), 20.
[39] Sam Wagner, Alan Pitz, Dan Zimmerman, and Bong Wei, "Interplanetary Ballistic Missile (IPBM) System Architecture Design for Near-Earth Object Threat Mitigation," Asteroid Deflection Research Center, Iowa State University, January 2009, accessed April 17, 2014, http://www.adrc.iastate.edu/files/2012/09/IAC-09.D1.1.1.pdf.
[40] Dearborn, Patenaude, and Managan, 3.
[41] Wei, 6.
[42] Ibid., 1.
[43] Dearborn, Patenaude, and Managan, 20.
[44] Ibid., 1.

nuclear device would explode microseconds later, effectively transmitting the full force of its energy to the asteroid.[45]

The yield of the nuclear device needed for a planetary defense mission would depend on a variety of factors, such as the size and composition of the threatening body and the amount of velocity change desired. To fully fragment a 1000-meter asteroid composed of silicate, research has shown that a nuclear explosion of 1.0 to 3.0 megatons is needed. To deflect the same asteroid a decade or more in advance of projected collision, a 300-kiloton stand-off blast would suffice.[46] Even successful fragmentation 15 days ahead of impact with Earth is possible for a 100-meter asteroid using a 100-kiloton device.[47]

In planning planetary defense missions, a margin of safety must be included to account for orbital perturbations. Although potential collisions with Earth can be estimated decades in advance, all objects traveling through space are subject to gravitational forces that can induce slight changes to their orbits. As asteroids and comets pass through the solar system they may experience small but disruptive gravitational pull from the planets, other asteroids, or the Sun.[48] The orbit of the asteroid Apophis is illustrative: it is projected to pass close to Earth in 2029 and 2036, but due to potential perturbations there are 146,500 kilometers of positional uncertainty – 23 times the radius of the Earth – for the 2036 passage.[49] Should an asteroid like Apophis need to be deflected, the total change in velocity induced must alter the orbit so that the asteroid misses Earth by a distance greater than the sum of the uncertainties, plus an additional safety margin.

Fully capable space launch systems will be essential for any planetary defense operation. As with nuclear weapons themselves, there currently are several space lift systems available, all of which have been rigorously tested, have proven reliability, and are capable of delivering the necessary nuclear device and support systems to intercept a threatening body. For example, the Delta IV Heavy launch vehicle, used by the Department of Defense to place national security assets into orbit, is capable of transporting more than 8400 kilograms of payload on an interplanetary trajectory. This is more lift capability than is needed to carry an American nuclear weapon, such as the B83 warhead, which weighs 1118 kilograms, along with requisite command, control, and telemetry systems.[50]

ISSUES AND CHALLENGES

The maturity of the U.S. nuclear weapons complex coupled with highly reliable and readily available space launch and control systems makes employment of a nuclear weapon for planetary defense a realistic option, with far less developmental risk than for the more exotic techniques that have been proposed. Only the use of a kinetic impactor poses fewer technical hurdles.

A nuclear mission would involve two basic acts: delivery of the weapon to the target, and the detonation. Direct delivery was demonstrated successfully in the July 2005 Deep Impact mission, in which an American robotic spacecraft was flown purposefully into the Tempel 1 comet, seen in Figure 4.[51] Nonetheless, new technological breakthroughs may be needed, particularly related to operating on or near the surface of an asteroid, for situations where a nuclear device would be placed on or buried beneath the asteroid's surface before detonation. The recent difficulties encountered by the European Space Agency's Philae spacecraft when

[45] Wei, 2.
[46] Holsapple, 115.
[47] Brian Kaplinger, Pavithra Premaratne, Christian Setzer, and Bong Wei, "GPU Accelerated 3D Modeling and Simulation of a Blended Impact and Nuclear Subsurface Explosion" (paper presented at the AIAA Guidance, Navigation, and Control Conference 2013, Boston, MA, August 19-22, 2013), 16.
[48] Wei, 3.
[49] Wagner, Pitz, Zimmerman, and Wei, 2.
[50] Ibid., 4-11 and Norman Polmar and Robert S. Norris, *The U.S. Nuclear Arsenal: A History of Weapons and Delivery Systems Since 1945* (Annapolis, MD: Naval Institute Press, 2009), 61.
[51] National Aeronautics and Space Administration, "Deep Impact," NASA Science, May 13, 2014, accessed June 27, 2014, http://science.nasa.gov/missions/deep-impact/.

landing on and anchoring to Comet 67P/Churyumov-Gerasimenko highlight the challenges of operating in a microgravity environment.[52]

Detonation has also been demonstrated. Prior to agreeing to a ban on the practice, in July 1962 the U.S. successfully exploded a 1.4 megaton warhead more than 240 miles above the Earth in a test called Starfish Prime, and the Soviet Union conducted its own thermonuclear explosion at extremely high altitude that same year.[53] These demonstrations quelled any doubts that a nuclear device would work in the harsh environment of space.

Operationally, warning time is a key parameter for planetary defense missions. With only a very small percent of the total population of potentially hazardous asteroids and comets currently known, it is very plausible that a threatening object will be discovered where there is little time for mitigation, in which case nuclear weapons may provide the only solution. One way to preserve a larger menu of mitigation options is to detect, catalog, and track the full population of PHOs in the solar system as early as possible.

While U.S. and international detection efforts have increased significantly over the past two decades, primarily through a network of civilian and government-operated observatories, the limitations of using terrestrial telescopes make this a very inefficient undertaking.[54] A massive advantage could be gained by employing a space-based telescope dedicated specifically for this purpose, as currently being planned by the nonprofit B612 Foundation, whose *Sentinel* spacecraft, scheduled for launch in 2018, is expected to identify up to 90 percent of all asteroids larger than 140 meters as well as a many asteroids as small as 30 meters in diameter.[55] Even with a much more comprehensive survey, however, there will not be complete coverage of the asteroid population and the appearance of a threatening comet could occur at any time, since many comets are in orbits lasting multiple hundreds or thousands of years – again potentially necessitating the use of a nuclear explosion as a last ditch, short-notice defense.

A second operational concern relates to the physical characteristics of many asteroids and comets. It will be difficult to determine the proper blast location and nuclear yield to defend against rubble pile, oddly shaped, binary, and rapidly rotating bodies. Further, for comets, the precise makeup of their nuclei is "among the more elusive questions of solar system science."[56] An attempt to deflect or fragment a threatening comet using the enormous impact of a nuclear explosion may inadvertently create large fragments with negligible dispersal velocity, potentially leading to several devastating impacts on Earth.[57] This supports the need for early detection as well as for conducting exploratory missions to threatening objects decades in advance of collision, in order to best ascertain their physical characteristics.

A third issue regards the possibility that a deflection or fragmentation effort could shower Earth with radioactive materials. The public has acute concerns over the dangers of radiation, which were on full display following the 2011 disaster at the nuclear power plants in Fukushima, Japan. From a scientific standpoint, the likelihood that any dangerous radiation from asteroid fragments or a poorly diverted object would pose a health threat on Earth is extremely small, and orders of magnitude less of a risk than posed by the fallout created during atmospheric testing of

[52] Peter B. de Selding, "European Spacecraft Touches Down on Comet," SpaceNews, November 12, 2014, accessed March 22, 2015, http://spacenews.com/42527european-spacecraft-touches-down-on-comet/.
[53] Gilbert King, "Going Nuclear Over the Pacific," Smithsonian.com, August 15, 2012, accessed April 12, 2014, http://www.smithsonianmag.com/history/going-nuclear-over-the-pacific-24428997/?no-ist.
[54] National Research Council, 29-50.
[55] B612 Foundation, "Sentinel Mission: Making the Map," B612 Foundation, January 2014, accessed March 22, 2015, https://b612foundation.org/sentinel-mission/.
[56] Paul R. Weissman, Erik Asphaug, and Stephen C. Lowry, "Structure and Density of Cometary Nuclei," in *Comets II*, ed. M.C. Festou, H.U. Keller, and H.A. Weaver (Tucson: the University of Arizona Press, 2004), 352.
[57] Wei, 3.

nuclear weapons in the 1950s and early 1960s.[58] Nonetheless, dealing with public perceptions and the vocal opposition that is likely to arise will be a significant aspect of any effort to employ nuclear weapons for planetary defense.

A final operational question surrounds command and control: what nation or nations will lead the mitigation effort against a threatening asteroid? Today, the answer is murky, as there are no agreed upon international conventions that directly address this issue. The primary source of international space law, the 1967 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies* (*Outer Space Treaty*), is silent on the issue of planetary defense, but does include guidance that could be deemed applicable. The treaty states as fundamental principles that the use of outer space is for peaceful purposes and for the benefit of all mankind, and that international cooperation is highly desired, particularly "in the interest of international peace and security."[59] This language, which was written decades before planetary defense became an issue in space policymaking circles, could be interpreted as supporting an international effort to mitigate a known asteroid or comet collision threat.

In 2013, in the spirit of the *Outer Space Treaty* and in reaction to the Chelyabinsk bolide, the United Nations Committee on the Peaceful Uses of Outer Space chartered a working group to evaluate potential mitigation schemes.[60] Nonetheless, there is no assurance that should a threat be identified, the UN will be able to muster international support for a mitigation mission. There is likely to be squabbling over leadership of the project and nonproliferation concerns over safeguarding weapons secrets, should a nuclear strike be the best or only option. Under such circumstances it may fall upon the shoulders of the United States or a likeminded group of nations to carry out on their own initiative a planetary defense operation. Since the 1990s, for example, Russia has made occasional overtures about working with the United States on nuclear planetary defense activities, although no concrete progress has been made toward a formal cooperative effort.[61]

There are also significant political and legal issues related to the use of nuclear explosions for a planetary defense effort. A plan to use nuclear weapons in space likely would face strident political and public opposition, based on the view that safer mitigation means would be available, and bolstered by restrictive language contained in the *Outer Space Treaty*.[62] Article IV of the treaty states that nations shall not "place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner."[63] Such unambiguous language makes no exception for defense of the planet. To address this hurdle in the face of a known threat, the language of the *Outer Space Treaty* could be revised, the UN could pass a resolution to provide an exception for the mission at hand, or the involved nations could work outside the purview of the treaty – all solutions that are bound to generate controversy.

In addition to the constraints of the *Outer Space Treaty*, other international agreements must be considered. Public outcry over nuclear testing and other events helped lead the United States, USSR, and United Kingdom to sign the Limited Test Ban Treaty in 1963, which prohibited nuclear explosions in space, as well as in the atmosphere

[58] Dearborn, Patenaude, and Managan, 20.
[59] I. Diederiks-Verschoor and V. Kopal, *An Introduction to Space Law*, 3rd ed. (New York: Wolters Kluwer, 2006), 161-162.
[60] United Nations Office for Outer Space Affairs, "Recommendations of the Action Team on Near-Earth Objects for an international response to the near-Earth object impact threat," Press Release, February 20, 2013.
[61] Kathy Gilsinan, "The Enemy of an Asteroid is My Friend, TheAtlantic.com, August 9, 2014, accessed March 22, 2015, http://www.theatlantic.com/international/archive/2014/08/asteroid-defense-us-russia-ukraine/375799/.
[62] Clark Chapman, "How not to save the planet," *New Scientist* 194, no. 2611 (July 7, 2007): 19.
[63] Diederiks-Verschoor and Kopal, 162.

and underwater.[64] This was followed by an international effort to implement a Comprehensive Test Ban Treaty (CTBT), which prohibited nuclear testing anywhere (although this treaty has neither entered into force nor been ratified, the United States voluntarily ended all explosive nuclear testing in 1992).[65] Should field testing or the use of a nuclear device for a planetary defense mission be necessary, it would require a significant change in U.S. policy, as well as that of other participating nuclear powers.

In the legal arena, a government seeking to use nuclear weapons for planetary defense must be prepared to address liability concerns. Under the *Outer Space Treaty* and the 1972 *Convention on International Liability for Damage Created by Space Objects*, the nation that launches an object into outer space "shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight."[66] This framework of strict liability could impact the decision to employ nuclear weapons, considering the tremendous financial risk for the launching state.

This risk takes many forms: the damage created by a failed launch, should the nuclear warhead land back on Earth; an unsuccessful deflection mission, where the asteroid or comet strikes the planet in a different location than originally forecast; and a fragmentation mission where a large piece of the target survives atmospheric friction and impacts the surface. To safeguard against liability hazards, a UN-chartered planetary defense mission could indemnify the launching and participating states from damages, or these states could choose to withdraw from the relevant treaties for the duration of the mission.

A final, long-term challenge surrounds the aspirational goal espoused by many world leaders, including the sitting U.S. President, to rid the planet of all nuclear weapons.[67] With thousands of bombs, warheads, and tactical weapons in existence, there is little likelihood that complete nuclear disarmament will occur in the near future. Still, should international consensus develop over time to winnow the world's nuclear arsenals, it is possible to foresee a future with drastically shrunken or completely expunged nuclear stockpiles.

In such a future, there may come a juncture where an asteroid or comet has been detected on a collision course with Earth, the threat cannot be addressed by non-nuclear means, and no nuclear weapons are available for deflection or fragmentation. This scenario would require the rebirth of a nuclear weapons complex and the development and manufacture of a new warhead – actions that could require critical time leading up to the projected impact.[68] To avoid this fate, maintaining a level of nuclear weapons capability to address possible planetary defense needs should be accounted for in future nuclear disarmament agreements.

CONCLUSIONS

The threat from collision by asteroid or comet is not a short-term issue, but one that will forever shadow the human species. There is no doubt that Earth will be struck by large asteroids or comets in the future. Only the timing is unknown.

No other currently feasible mitigation technique provides the high levels of energy needed for asteroid deflection or fragmentation as the detonation of a nuclear weapon. While non-nuclear slow push or kinetic impact methods may be suitable for smaller asteroids or those detected decades before collision, it is likely that a nuclear explosion will be the only adoptable solution for fending off the largest threatening bodies or where an inbound asteroid or comet is first identified

[64] Walter A. McDougall, *... The Heavens and the Earth* (Baltimore: The Johns Hopkins University Press, 1985), 273-274.
[65] Office of the Secretary of Defense, 5.
[66] Diederiks-Verschoor and Kopal, 174.
[67] Barack Obama, "Remarks by President Barack Obama," speech delivered Prague, Czech Republic, April 5, 2009, The White House, accessed April 15, 2014, http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered.
[68] Dearborn, Patenaude, and Managan, 21.

with little time before impact.

For future generations, new technologies may displace nuclear weapons as a tool for planetary defense. The use of directed beams of neutral particles could in theory be transmitted over extremely large distances to ablate the surface of an asteroid. Chemical or biological compounds or mechanical 'eaters' might be developed to consume enough of an asteroid's physical structure to render it harmless when it strikes the Earth's atmosphere. Equally compelling, should methods be devised to contain and store it, small quantities of anti-matter could be used either as a strong explosive or to propel the threatening body to a safe orbit.[69]

These techniques, however appealing in theory, are generations away from development, if at all. With today's technology, it is a simple truth that the use of a nuclear device to prevent collision with Earth of a large asteroid or comet remains the most effective solution in a wide range of scenarios. The operational, legal, political, and public perception challenges related to the use of nuclear weapons to defend against a hazardous space object are vast, but must be addressed and overcome if nuclear weapons become necessary for planetary defense.

The development of nuclear weapons has been seen by many as a tragic turn in history, unleashing for the first time the potential power to destroy human civilization. How extraordinary it would be, then, if a monstrous asteroid on a collision course with Earth – the same primordial force of nature that exterminated the dinosaurs and that today could eliminate humanity – was deflected from its orbit by the well-timed impulse of a man-made thermonuclear explosion.

Rather than act as the destroyer of mankind, nuclear weapons would serve as its most vital defender.

[69] Gritzner and Kahle, 183-184.

Figure 1. Trees felled by the 1908 Tunguska explosion. Photo courtesy of the Leonid Kulik Expedition.

Figure 2. Aerial view of the Manicouagan impact crater, Quebec, Canada. Roughly 100 kilometers wide, this crater was created more than 200 million years ago when an asteroid estimated at five kilometers in diameter struck Earth. Photo courtesy of NASA/Near Earth Object Program.

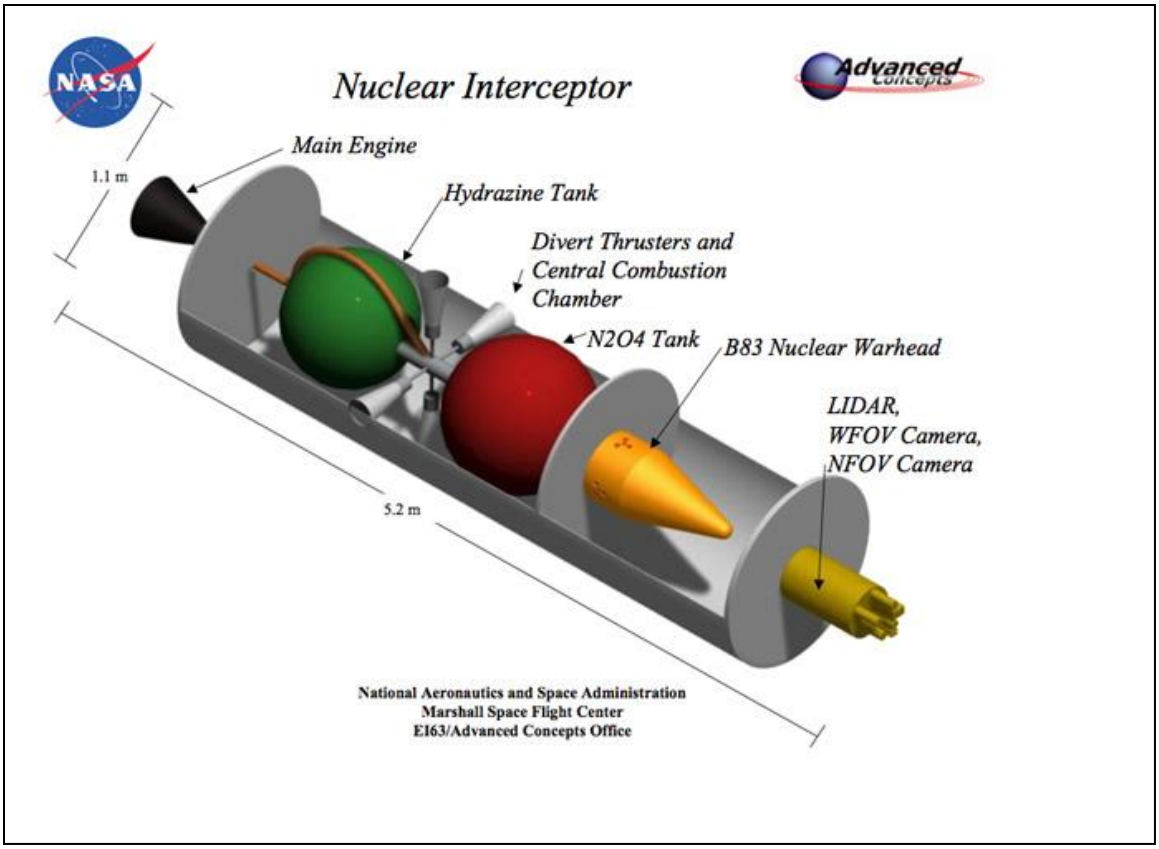


Figure 3. NASA nuclear interceptor concept, developed in 2007 and suitable for use in stand-off or surface detonations to deflect a threatening asteroid or comet. The B83 warhead has a programmable yield of up to 1.2 megatons. Image courtesy of NASA/Marshall Space Flight Center.

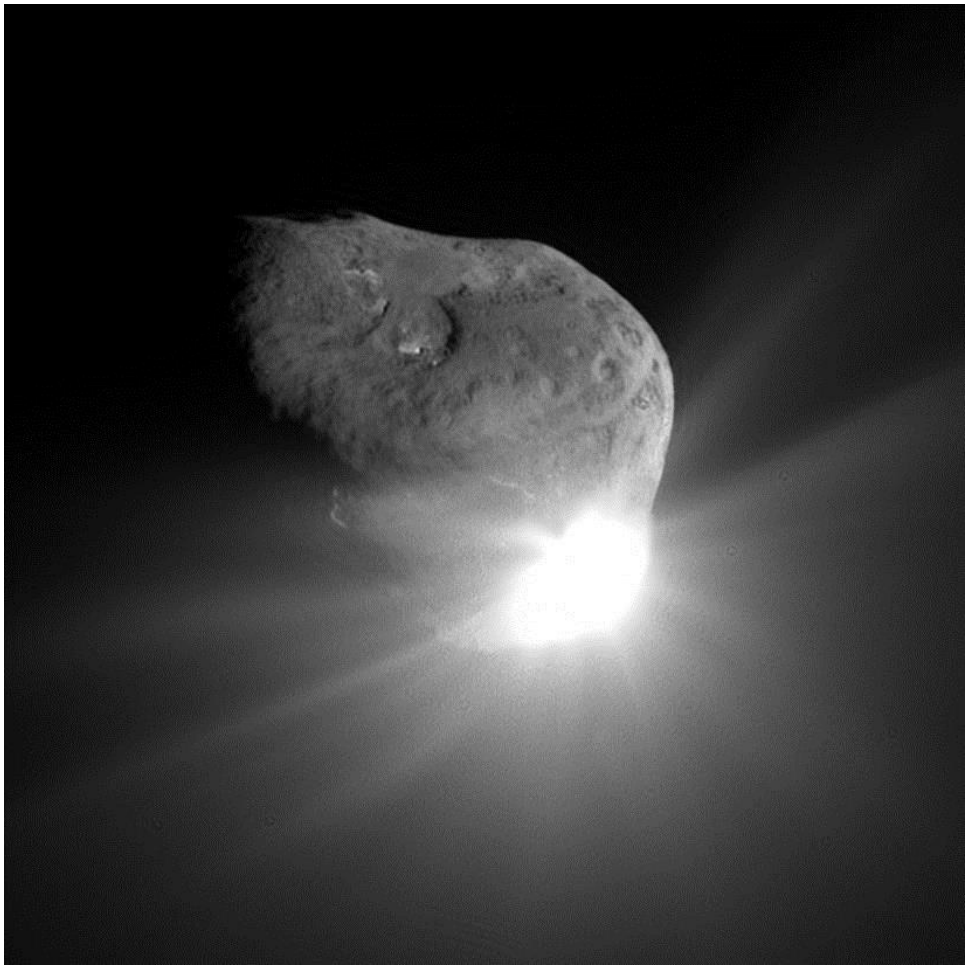


Figure 4. Comet Tempel 1 after being struck by the Deep Impact space probe in July 2005. Photo courtesy of NASA/Jet Propulsion Laboratory.

Cyberwar: Clausewitzian Encounters

Marco Cepik, Diego Rafael Canabarro, and Thiago Borne Ferreira

As Clausewitz's masterpiece suggests, language matters for how states conceptualize and plan for war. 'Cyberwar', now on the lips of nearly every national security policymaker, may turn out to be a misnomer.

The Digital Era and the spread of contemporary information and communication technologies (ICT) bring about different challenges for national and international security policymaking, heating up academic and political debate over the scope and the implications of an upcoming cyberwar.[1] This article evaluates three well-known assertions related to this highly controversial issue. The first section defines the concept of cyberwar according to its original employment. The second section presents each controversial assertion synthesized from qualitative content analysis of selected academic publications, landmark documents, and news accounts. The three of them are, respectively: (a) cyberspace is a new operational domain for war; (b) cyber warfare can be as severe as conventional warfare; and (c) cyber warfare can be waged both by state and non-state actors. In the third section we evaluate them collectively through theoretical and empirical lenses. The final section consolidates findings, indicating paths for further inquiry and policy caveats.

This text deliberately evokes an idea employed in the past by other accounts of the phenomenon (Tennant, 2009; Morozov, 2009; Greenemeier, 2011; Valeriano; Maness, 2012). The reference has two justifications. First, it seeks to reconnect the concept of cyber warfare to its Clausewitzian roots, highlighting the ambiguous role of information in war and the need to treat cyberspace as an integral part of the political and strategic realms, not as a completely separated domain. Second, it aims at the importance of careful evaluate propositions about the securitization of cyberspace.

[1] Marco Cepik is Associate Professor, Federal University of Rio Grande do Sul (UFRGS); Diego Rafael Canabarro, Ph.D., is Special Advisor to the Brazilian Internet Steering Committee (CGI.br); Thiago Borne Ferreira, is a Ph.D. candidate in International Strategic Studies, Federal University of Rio Grande do Sul (UFRGS).

WHAT IS CYBERWAR?

The book chapter entitled *Cyberwar is coming!* by John Arquilla and David Ronfeldt (1997) is directly responsible for the formal incorporation of cyber to the lexicon of Security and Strategic Studies. According to the authors, "a case [existed] for using the prefix [from the Greek root *kybernan*, meaning to steer or govern, and a related word *kybernetes*, meaning pilot, governor, or helmsman] in that it bridges the fields of information and governance better than does any other available prefix or term," such as, for instance, information warfare (Arquilla; Ronfeldt, 1997:57).

Information warfare should be treated as a subfield of larger information operations, which "comprise actions taken to affect adversary information and information systems while defending one's own information and information systems." Information warfare is a more restrictive concept: it refers "to those information operations conducted during times of crisis or conflict intended to affect specific results against a particular opponent" (Schmitt, 1999:07).

The broad concept of information operations includes electronic warfare (EW), psychological operations (PSYOPS), computer network operations (CNO), military deception, and operations security (Zimet; Barry, 2009:291). Because of the ambiguous role of information in war (Clausewitz, 2007, Book I, Chapter VI), "information operations have been recognized as a

distinct form of warfare meeting its own separate doctrine, policy, and tactics," (Schmitt, 1999:32)[2].

Therefore the use of the prefix "cyber" in this context was intended to comprise both the role of digital computers and computerized networks from a technological perspective as well as the organizational and institutional consequences of their application on information gathering, processing and sharing. The authors allegedly tried to catch-up with "some visionaries and technologists who [were] seeking new concepts related to the information revolution" (Arquilla; Ronfeldt, 1997:59).

Basically, we agree with a conceptual definition of cyberwar that refers to the control of information-related factors in the preparation and waging of war. Cyberwar is conducted through the development and deployment of different technologies (increasingly robotic and digital in nature), as well as through the implementation of changes in military organization and doctrine. In this sense, "cyberwar is about organization as much as [it is about] technology" in order to "turn knowledge into capability" (Arquilla; Ronfeldt, 1997:30). The same is valid today, with proper qualifications and caveats.

Highlighting the societal implications of the information revolution[3], Arquilla and Ronfeldt also introduced the broad concept of netwar: a sort of non-military information-related multidimensional conflict, that could be waged by state and non-state actors with a wide range of available tools (public diplomacy, propaganda, interference with local media, the control of computer networks and databases, etc.), with the purpose of "trying to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it" (Arquilla; Ronfeldt, 1997:28). According to Arquilla and Ronfeldt's framework, despite being non-military in essence, netwar campaigns may deal with military issues such as nuclear weapons, terrorism, etc. Netwars may also escalate to the level of cyberwars when they affect military targets. Moreover, they can be employed in parallel to both conventional and cyber war.

More than twenty years later, cyber has become increasingly identified with the pervasiveness of cyberspace: "an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures" (Kuehl, 2009:28)[4].

In the military, information and intelligence operations, routine administrative functions, and a wide array of everyday jobs have been increasingly developed and transformed with the support of interconnected electro-electronic devices (Zimet; Barry, 2009; Libicki, 2012; Rid, 2012a). The same applies to the civilian sector (Blumenthal; Clark, 2009; Kurbalija; Gelbstein,

[2] Schmitt affirms that the terms information and information systems "shall be understood very expansively [...] The United States military defines information as 'facts, data, or instructions in any medium or form' and an information system as the 'entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information" (Schmitt, 1999:07).

[3] The whole field of Digital Era studies was influenced by *The Rise of the Network Society* (1996), where Manuel Castells first recognized that the "ability to use advanced information and communication technologies […] requires an entire reorganization of society" to cope with the decentralized character of networks that give shape to societies in an information age (Castells, 1999:03). Both cyberwars and netwars are founded upon the premise that ICTs entail networked forms of organization: the first category referring specifically to the military sector; the latter to the civilian sector at large. Nonetheless, the labeling of inherently non-military phenomena as "war" can also lead to unjustified events of securitization (Hansen; Nissenbaum, 2009).

[4] It is interesting to note that cyberspace was not a defining character of cyberwars to Arquilla and Ronfeldt. According to them cyberspace is "another new term that some visionaries and practitioners have begun using" to refer "to the new realm of electronic knowledge, information, and communications – parts of which exist in the hardware and software at specific sites, other parts in the transmissions flowing through cables or through air and space" (Arquilla; Ronfeldt, 1997:59).

2005). In the last two decades cyberspace has been greatly enlarged mainly as a result of the steady growth and spread of the Internet and interrelated technologies (Joint Chiefs of Staff, 2013:v). Currently, the Internet is the main entry door for cyberspace, mainly because the convergence of "all modes of communication – voice, data, video, etc. – on the Internet platform" (Mueller, 2010:129) has gradually blurred the lines between cyberspace and the Internet.

In this sense, the first decades of the 21st Century are defined by the growing importance of the technological and organizational aspects of cyberspace politics. Consequently, cyber-related issues increasingly permeate the agenda of national and international security (Weimann, 2004; O'Harrow, 2005; Nissenbaum, 2005; Eriksson; Giacomello, 2007; Kramer; Starr, 2009). As examples, one could just mention the public debate around increasing reliance of criminal and terrorist organizations on Internet-based applications (e.g. the Web, electronic mail, chat servers, social networks); the major assaults on Estonia (2007) and Georgia (2008) carried through Internet-based technologies and applications; the spread of malicious computer codes with unprecedented characteristics and outcomes, such as Stuxnet, Flame, and Gauss (2012); some alleged State-sponsored violations of sensitive political and economic databases, as well as public social networks profiles, such as the attacks reported by CitizenLab to computers associated with Dalai Lama (2008), the stealing of Sony movies and classified documents (2014), and the US Cyber Command Twitter account breach (2015); the Snowden affairs (2014), which publicized documented details of mass-surveillance programs developed mainly by the US National Security Agency; and the actions of civil society organizations such as Wikileaks and Openleaks, as well as hacktivists groups that employ Internet applications as means for political activism, such as Anonymous and Lulzsec.

Because of the need for promptly tackling these different perceived threats from a practical perspective, the theoretical notion of "cyber" as something related to the complex interactions between technology and networked governance has become subordinated to a narrow conception of "cyber" as something identified with the technical and tactical exploitation of cyberspace. As a detailed survey of the database compiled by Harvard's Berkman Center for Internet and Society (The Berkman Cybesecurity Wiki) reveals, the bulk of intellectual background for policy and legal development has been mainly produced by security related governmental agencies and IT corporations. Of course, we have no feud against government or the private sector getting involved in public debates about cyber warfare. Our point here is to stress the need to take a broader, theoretically oriented, political and societal perspective when trying to assess the meaning of cyberspace for national and international security policymaking.

More specifically, critical debate on basic concepts is crucial to avoid analogies without real theoretical or empirical grounds (Libicki, 2012). Therefore, it is a good sign that scholars recently began advancing more rigorous and consistent analyses of publicly known cyber events (Rid, 2013; Deibert, 2013; Gray, 2013; Demchak, 2012). Their works question taken-for-granted normative propositions on cyberwar. At the same time, they delve into the severity and the sophistication of contemporary cyber operations of all sorts.

THREE CONTROVERSIAL CLAIMS ABOUT CYBERWAR

In order to contribute to a more balanced account of cyberwar, the following paragraphs summarize three common assertions related to the phenomenon. These three were selected from academic publications, landmark documents and news accounts covering the years 2012 and 2013.[5]

[5] The main sources were: (1) the digital database of the Center for International Studies on Government (CEGOV), compiled mainly through the CAPES Foundation Portal, as well as the physical libraries at UFRGS; (2) the physical and digital inventories of the University of Massachusetts, Amherst; and (3) the Cybersecurity Wiki maintained by the Berkman Center for Internet and Society of Harvard Law School, which consists of "a set of evolving resources on cybersecurity, broadly defined, and includes an annotated list of relevant articles and literature". It is available at: http://cyber.law.harvard.edu/cybersecurity/Main_Page (accessed August 18, 2014).

Our goal in debating them is not to dismiss them or prove them entirely false, but to call for a better-established scope of validity. After presenting each of them separately in this section, we shall discuss them collectively in the next section.

"Cyberspace is a new operational domain for war"

Referring to cyber-related incidents as warfare in the fifth domain has become a standard expression over the last ten years. "Cyberspace is a new theater of operations," says the 2005 US National Defense Strategy. "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare […] just as critical to military operations as land, sea, air, and space," wrote the former US Deputy Secretary of Defense William Lynn (2010) in *Foreign Affairs*. "Warfare has entered the fifth domain: cyberspace," alerted The Economist in the same year (*The Economist*, 2010). Indeed, comparable claims have been widely spread in the past years, and the idea has reached politicians, intellectuals, the military, and the media all around the globe.

In 2012, the popular Argentinean *DEF Magazine* defined cyberspace as "a new battlefield" (Lucas, 2012). The idea was reaffirmed by an Argentinean official in the same year: "electronic warfare relates to more traditional domains of conflict: land, sea, and air. Cyberwar is undertaken in a new domain of hostility among nation-states" (Uzal, 2012).

"Cyber warfare can be as severe as conventional warfare"

According to the 2010 Brazilian Green Book on Information Security, "natural threats (posed by forces of nature) or intentional ones (sabotage, crime, terrorism, and war) acquire a greater dimension when the use of cyberspace is involved". During the III International Seminar on Cyber Defense held in Brasilia in 2012, the Brazilian Minister of Defense reaffirmed the idea, urging Brazil and other countries to get ready to face a new cyber-related threat capable of bringing harmful consequences to society at large.

In 2011 the *Washington Post* reported: "a cyber attack against Libya […] could have disrupted Libya's air defences but not destroyed them. For that job, conventional weapons were faster, and more potent. Had the debate gone forward, there also would have been the question of collateral damage. Damaging air defence systems might have, for example, required interrupting power sources, raising the prospect of the cyber weapon accidentally infecting other systems reliant on electricity, such as those in hospitals" (Nakashima, 2011).

One year later the same newspaper stated that "over the past decade, instances have been reported in which cyber tools were contemplated but not used because of concern they would result in collateral damage […] There is the danger of collateral damage to civilian systems, such as disrupting a power supply to a hospital" (*Washington Post*, 2012).

The already mentioned Argentinean *DEF Magazine* also suggested in 2012 that "a new sort of conflict is dominating the world stage: cyberwar. It doesn't matter the size and the available resources of the opponents. With an adequate IT capacity, the aftermath can be lethal and irreparable" (Noro, 2012).

"Cyber warfare can be waged both by state and non-state actors"

The 2003 US National Strategy to Secure Cyberspace alerts: "because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against our infrastructures and cyberspace." This notion is further developed by the 2012 DoD Priorities for 21st Century Defense: "both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland".

Harvard Law School Professor, Jack Goldsmith, summarizes these perceptions as follows:

> "Taken together, these factors – our intimate and growing reliance on computer systems, the inherent vulnerability of these systems, the network's global nature and capacity for

> near instant communication (and thus attack), the territorial limits on police power, the very high threshold for military action abroad, the anonymity that the Internet confers on bad actors, and the difficulty anonymity poses for any response to a cyber attack or cyber exploitation – make it much easier than ever for people outside one country to commit very bad acts against computer systems and all that they support inside another country. On the Internet, states and their agents, criminals and criminal organizations, hackers and terrorists are empowered to impose significant harm on computers anywhere in the world with a very low probability of detection" (Goldsmith, 2010).

On the other hand, Dorothy Denning, Professor at the Naval Postgraduate School, is more doubtful. She contends that:

> "There are several factors that contribute to a sense that the barriers to entry for cyber operations are lower than for other domains. These include remote execution, cheap and available weapons, easy-to-use weapons, low infrastructure costs, low risk to personnel, and perceived harmlessness. [...] Cyber weapons are cheap and plentiful. Indeed, many are free, and most can be downloaded from the Web. Some cost money, but even then the price is likely to be well under US$ 100,000. By comparison, many kinetic weapons, for example, fighter jets, aircraft carriers, and submarines, can run into the millions or even billions of dollars. Again, however, there are exceptions. Custom-built software can cost millions of dollars and take years to develop, while kinetic weapons such as matches, knives, and spray paint are cheap and readily available" (Denning, 2009).

As core propositions in the current debate regarding cyberwar, the three claims just presented cannot either be accepted or dismissed without strong empirical and logical tests, both beyond the scope of this article. However, in order to better define their scope of validity and the risks involved in accepting them as unqualified truth, we shall evaluate them collectively from the standpoint of a scientific research program such as Clausewitz's theory of war.

TOWARDS A CLAUSEWIZIAN CONCEPT OF CYBERWAR

We shall depart from Betz's perception that cyberwar is a "portmanteau of two concepts": "cyberspace and war, which are themselves undefined and equivocal; it takes one complex non-linear system and layers it on another complex non-linear system […] As a result, it does not clarify understanding of the state of war today; it muddies waters that were not very transparent to start with" (2012:692). Hence we need to clearly define each concept before integrating them, starting with cyberspace.

Allow us to recall Kuehl's (2009) definition presented in the first section: cyberspace is "framed by the use of electronics and the electromagnetic spectrum." It is employed "to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures." Despite one's natural impetus to interpret interconnected ICTs as synonymous with Internet, cyberspace is a much more complex environment composed by many different systems. "At the very least yours, theirs, and everyone else's", says Libicki (2012:326).

Considering hypothetical actors A and B, this idea can be represented in graphical terms, as in Figure 1.

Both actors own closed (air-gapped) information systems (represented on circles A.1 and B.1); they also own systems (circles A.2 and B.2) that more or less overlap with global open communications backbones (GOBC) such as telecom lines, the radio spectrum, the Internet, etc. (represented on circle GOBC.3). Naturally, A and B can also have overlapping systems between themselves and/or between each one and other actors (circles A.3, B.3, and C.3). These systems can also be more or

less connected to global open communications backbones (in this case, directly through B.3).

All of these systems – mounted over a variable set of infrastructure, logical, and application layers – can be some way or another interconnected. The interconnection can be permanent and synchronous (such as in the case of Internet-based connections), as well as intermittent and asynchronous (such as in the case of software updating or in the use of a flash drive to exchange information between computers). Even when there are no digital bridges that allow access to a specific system, the isolation "can be defeated by those willing to penetrate physical security perimeters or by the insertion of rogue components. But efforts to penetrate air-gapped systems are costly and do not scale well" (Libicki, 2012:326).

As stated before, society relies on the correct performance of information systems for a myriad of more or less vital purposes. As man-made creations, information systems, and consequently cyberspace, have inherent flaws and vulnerabilities (Stamp, 2011; Kim; Solomon, 2010). Thus, the more one relies on them, the more it is potentially threatened by the eventual exploitation of the systems' vulnerabilities.

Nonetheless, we agree with Martin Libicki (2012) in highlighting that cyberspace is not a domain that can be isolated from others exactly due its pervasiveness to all human activities. In this sense, cyberspace can be treated as a separated warfighting domain only for logistical and command and control purposes, and even this trend could be argued against. However, it is more important to accurately communicate to the armed forces and the citizens that physical and logical realities of cyberspace are much harder to separate from land, water, air, and outer space than each of these other four domains can be separated from each other. Moreover, the whole concept of jointness depends, to become reality, on acknowledging the pervasiveness of cyberspace.

Since it is not correct to fully equate Internet with cyberspace, or treat cyberspace as something that can be isolated from the whole contemporary social fabric, there are operational implications when war reaches cyberspace. As Martin Libicki said regarding his conceptual framework for offensive and defensive cyber capabilities:

> "The more these tasks require correct working of the systems, the greater the potential for disruption or corruption that can be wreaked by others. Similarly, the more widely connected the information systems, the larger the population of those who can access such systems to wreak such havoc. Conversely, the tighter the control of information going into or leaving information systems, the lower the risk from the threat" (Libicki, 2012:323).

Following this idea, offensive actions in cyberspace aim at exploiting systems' flaws and vulnerabilities to "interfere with the ability of their victims to carry out military or other tasks, such as production" (Libicki, 2012:323). It is in essence a matter of reconnaissance, exploration, and exploitation of an opponent's entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Defense, on the other hand, involves a complex set of preventive and reactive actions in order to secure the systems (Clark; Levin, 2009). They comprise engineering and organizational decisions related to the situational environment, the set of technologies employed, and the degree of connectivity (to other systems) and openness (to a range of users) of a specific system. They also involve the permanent monitoring of the information flowing through the system, and its operation and functioning according to given parameters.

To be effective, the exploration/infiltration phase of a given attack has to be supplemented by the development of other code-based tools for disrupting the infiltrated system. However, the window of opportunity for infiltration and disruption is generally very narrow after vulnerability is discovered. Once an attack is detected, the target system can be adapted to tackle the threat. The number of different information systems and their potential lack of

structural uniformity (shown in Figure 1) mean that the strategic preponderance of defense over offense is not easily overturned. In other words, there are so many engineering options available for information systems' designers that the development of cyber offense capabilities might be way too expensive and ineffective to be translated into a strategic advantage.

In this sense, most offensive cyber actions are hard to repeat in patterned operational fashion: "once the target understands what has happened to its system in the wake of an attack, the target can often understand how its system was penetrated and close the hole that let the attack happen" (Libicki, 2012:323). Furthermore, as sensitive ICT systems generally entail great amounts of customization, the development of ready-made, mass-produced cyber weapons might be useful only for a few publicly open interoperable systems. The development of custom cyber weapons not only demands great amounts of resources (intelligence, funding, working-hours, etc.), but also means that the more customized the cyber weapon, the narrower its scope of application (Rid, 2013).

On the other hand, one might still affirm that the greater the Internet reliance, the greater the homogeneity of IT solutions and the greater the risks inherent to interconnectivity. Despite the suggestion that interconnectivity can lead to systemic hazardous events, vital information systems tend to be – and are increasingly becoming – more and more redundant and resilient (Sommer; Brown, 2011).

Actually, there is no such thing as a static cyberspace, neither in physical (infrastructure) nor in virtual (code) terms. To borrow a Clausewitzian term, cyberspace is a chameleon: its mutations depend on the decisions taken by individual information systems' owners. Therefore, calling cyberspace an operational domain without proper qualification entails the risk of overshadowing the inherent malleability of its components and consequently stresses the need of deploying permanent and vigilant tools for "perimeter" monitoring instead of making safety and security engineering/governance a priority when it comes to defense.

When it comes to offense, the development of general-purpose capabilities also needs to be balanced against the political and economic costs of exploiting (physically and digitally) the bulk of other actors' systems, as highlighted by the Snowden affair and the following diplomatic chorus of disapproval. This is not to say that cyberspace is not relevant for security and defense policymaking. On the contrary, it is a way to mind the fact that a large amount of resources might have been applied to suboptimal alternatives for ensuring national security – due to the hubris involved in treating as a self-contained operational domain something as ubiquitous and pervasive as cyberspace. That trend might be even more severe during times of economic or political distress, and might have negative outcomes if great powers develop a preemptive approach towards each other and third countries.

Regarding the second claim, that cyberwar can be as severe as conventional warfare; we first need to define the concept of war. According to Clausewitz, (1) war is never an isolated act, (2) war does not consist of a single blow, and (3) in war the result is never final (Clausewitz, 2007:17-19). Furthermore, as Clausewitz (2007:13) also reminds us, "war is […] an act of force to compel our enemy to do our will". The ultimate consequence of this prerogative is that war is necessarily violent. Potential or actual use of force, in Clausewitz's thinking, is the fundamental aspect of all war. Actually, violence plays a central role in his 'wondrous trinity' (*wunderliche Dreifaltigkeit*), which is made up of reason, natural force, and chance. The unifying concept of war in Clausewitz encompasses singular motives and dynamics that yet form an indivisible whole (Echevarria, 2007:69-70).

From a material point of view, every act of war is always instrumental to its ends. There has to be a means – physical violence or the threat of force – and there has to be an end – to impose one's will on the enemy. To achieve the end of war "the opponent has to be brought into a position, against his will, where any change of that position brought about by the continued use of arms would bring only more disadvantages for him, at least in that opponent's view" (Rid, 2012a:08). In this

sense, actual violence in actual wars does not easily escalate towards the logically possible extreme because of its instrumental and interactive nature.

Denial of service attacks such as those perpetrated by groups like Anonymous to take down or deface websites tend to be easily remedied or counteracted by the victims. And the bulk of scams that have been happening in the last years through ICT systems do not aim at exercising political power over an enemy, but only to exploit information for illegal commercial purposes. Intelligence related operations through cyberspace are obviously related to power struggles, but they are not warfare. In short, no testified cyber attack has ever caused a single casualty, injured a person, or severely damaged physical infrastructure. Taking this very characteristic alone before analyzing Clausewitz's prerogatives further, it seems exaggerated (or at least precipitate) to treat code-triggered consequences as equal to kinetic violence. "Violence in cyberspace is always indirect", says Rid (2012b).

It means that ICT systems first have to be weaponized in order to produce physical and functional damage to people, infrastructure, and organizations. One could arguably say that code weaponizing is exactly what is happening right now in the realm of international security; physical harm would be only a matter of time or disclosure about what is going on. Maybe, but empirical public evidence so far does not corroborate the second claim.[6]

Besides, it is hard to sustain at this point that any cyber attack reported so far has irrefutably forced the target to accept the offender's will. Nonetheless, that might not be the case if one considers the potential massive social-psychological risk inherent to the consequences of having governmental and banking web servers shutdown; personal and financial data stolen from cloud computing providers; SCADA systems unexpectedly operating anomalously without proper technical explanation as they did in the Stuxnet event; things from satellites to webcams and computer speakers turning on and off randomly and without direct user control, etc.

As Thomas Rid recognizes: "Cyber attacks, both non-violent as well as violent ones, have a significant utility in undermining social trust in established institutions, be they governments, companies, or broader social norms. Cyber attacks are more precise than more conventional political violence: they do not necessarily undermine the state's monopoly of force in a wholesale fashion. Instead they can be tailored to specific companies or public sector or organizations and used to undermine their authority selectively" (Rid, 2013:26).

The reiteration and persistence of non-violent cyber attacks (in isolation or in combination with other offensive activities short of war), coupled with the ever going preparation for responding to and retaliating cyber attacks in different political playing fields could escalate tensions up to the point of full-blown violent conflict. This possibility, as logical as it may be, has to be reconciled with some empirical corroboration before any government or armed force start to treat cyber incidents as equivalent of using kinetic or direct-energy weapons.

Finally, there is the risk of treating "the cyber" as another technological tool that would easily give the offensive a brutal advantage in war. "Technology has always driven war, and been driven by it [...] and yet the quest for technological superiority is eternal", explains Van Creveld (2007). For instance, in the 1930s and 1940s, air force superiority was thought to be the decisive feature for winning a war. In the 1990s, air force superiority was coupled with microelectronics in the development of precision-guided ammo, which would avoid the excessive loss of money and lives in war. The development of unmanned aerial vehicles (UAVs) follows that trend. "The problem is that when [people] talk of

[6] To be fair, Thomas C. Reed's memoir book *At the Abyss* (2005) describes how an American covert operation allegedly used malicious software to cause an explosion in Russia's Urengoy–Surgut–Chelyabinsk pipeline back in 1982. The incident might have caused casualties, even though there are no media reports, official documents, or similar accounts to confirm Reed's allegation. Also, it is not settled whether the Stuxnet attack caused destruction to the Iranian nuclear centrifuges, or if it only rendered them inoperative.

'stand-alone' cyberwars they are arguing a theory of a new form of war in which decisive results are achieved without triggering the thorny problem of escalation" – says Betz (2012:696).

Against the idea of a "cyber silver bullet" stands Clausewitz's third fundamental element of war: its political and interactive nature. According to him, warfare is "the continuation of politics by other means" (Clausewitz, 2007:28) because politics is the ever-open interaction of wills among individuals and political entities with potential contradictory ends, whatever constitutional form such polities may have. Individuals, groups, and polities have intentions (or emotional desires) to be transmitted to (and understood by) the adversary at some point during the conflict.

In contrast, Richard Clarke (2010:67-68), for instance, describes a hypothetical overwhelming cyber attack on the United States "without a single terrorist or soldier ever appearing". Addressing Stuxnet, Michael Gross wrote for *Vanity Fair* in April 2011: "[this] is the new face of 21st-century warfare: invisible, anonymous, and devastating". This brings us back to the problem of attribution and to the third controversy, regarding state and non-state actors alike being able to wage cyber warfare.

There is no doubt some cyber incidents are hard to publicly attribute to a specific actor, even if many have been increasingly political in nature or indirectly connected to political events. The Web War in Estonia is allegedly related to the government's discretionary removal of a Soviet-era statue from downtown Tallinn. The cyber attacks against Georgian official websites preceded the 2008 Russia-Georgia War. Some other attacks present political motivation, having been carried on by groups such as Anonymous, LulzSec, and others. The "Operation Payback", so far the largest operation coordinated by Anonymous, was aimed at disrupting online services of organizations that work in favor of copyright and anti-piracy policies, such as the Swedish Prosecution Authority, the Motion Pictures Association of America (MPAA), the International Federation of Phonographic Industry (IFPI), the Recording Industry Association of America, a large number of Law Firms, as well as individual American politicians, like Gov. Sarah Palin or Sen. Joseph Lieberman. That operation escalated to "Operation Avenge Assange" and started targeting the different companies and governments involved in the financial siege imposed on Wikileaks and the criminal prosecution unleashed against Julian Assange. The operations comprised website defacements, distributed denial of services attacks, leaks of classified information, and so on.

But they have not been translated into violent acts of any nature. Also, it is hard to establish the real cohesion and political power of these groups, for they seem to lack much common ground, put aside an ideological identity, for their activities. According to Betz (2012:706), "the means for them to exert noteworthy power – to compel, or attempt to compel, their enemies to do their will are available and growing in scale and sophistication. […] [Nonetheless] no networked social movements as of yet have attached existing, albeit new, ways and means to an end compelling enough to mass mobilize." A clear example of that lack of critical mass and political cohesion is reflected in the generally known rivalry and competition between Anonymous and LulzSec (Fogarty, 2011), which became dramatic after a leader of the first (and probably founder of the second) was arrested by the FBI and turned in a lot of "Anons" in exchange for clemency and legal benefits (Roberts, 2012; Biddle, 2012).

It is reasonable to argue that it is difficult to sustain the idea that such groups match state-like capabilities. It is also hard to establish the level of allegiance, competence, and cohesion (*esprit de corps*) among their ranks. Even so, there is scant if any evidence that actors other than states - for now at least - do have capabilities to harm and continuously cause havoc through digital means. As it will be shown below, treating the actions perpetrated by such groups as military operations, or even as terrorist activities in cyberspace might be dangerous for democracy without allowing clear improvement in security levels.

Sure, even non-state actors could employ cyber attacks as part of a larger operation also involving direct political violence. However, such actions might be best captured by terms such as sabotage,

espionage, subversion, or even terrorism in a more extreme possibility (Rid, 2013). The notion that non-state actors can wage cyberwar properly defined resemble the once popular notion that non-state actors were capable of developing and using weapons of mass destruction in a sustained confrontation against states. One can imagine a scenario where a highly organized, rich, secretive and skilled non-state actor could acquire one such weapon and use it, but even that is not the same as waging chemical, biological, or nuclear war. In short, Clausewitzian criteria provide a better framework to assess cyber events and actors and decide if they are instantiations of war or something else. The Clausewitzean scientific research program is capable of incorporating and explaining such heuristic novelty represented by the concept of cyberwar in the 21st Century.

CONCLUSION

The controversies explored above not only encompass conceptual aspects of warfare, but also delve into some practical implications that are relevant for the overarching policy cycle in different countries. In sum, they highlight the political, economic, and societal trade-offs that are involved thereon. This article argues for a more precise and circumscribed concept of cyberwar that is better for addressing the phenomenon at various levels of concern and planning, related to both national and international security.

As Collier and Mahon (1993:845) remind us, "stable concepts and a shared understanding of categories are routinely viewed as a foundation of any research community. Yet ambiguity, confusion, and disputes about categories are common in the social sciences". The perpetual quest for generalization and the effort to achieve broader knowledge generate what Sartori (1970; 1984) called conceptual traveling (the application of concepts to new cases), but also may cause conceptual stretching (the distortion that occurs when concepts do not fit the new cases). According to him, understanding the proper scope of validity of a concept (the set of entities in the world to which it refers) as well as its intention (the set of meanings or attributes that define the category and determine membership) is essential in order to avoid overstretching. While the use of cyberwar is a recurrent rhetorical trope in public debates, it demands more than heat and loudness to call for the attention it deserves. Democracy and security can only be preserved and nurtured by serious consideration of the consequences and proper scope of political concepts, along with their policy implications.

Childress (2001:181), for example, provides an interesting view on the morality of using the language of warfare in social policy debates: "in debating social policy through the language of war, we often forget the moral reality of war. Among other lapses, we forget important moral limits in real war – both limited objectives and limited means". Childress however is not suggesting that one should avoid metaphors at all. However, the loose use of the metaphor of cyberwar, for instance, might not only lead to the aforementioned conceptual stretching, but also to improper or ineffective responses.

Consider for instance two widely adopted categorizations of cyber threats and cyber conflicts. The first one categorizes cyber terror, hacktivism, black hat hacking, cyber crime, cyber espionage, and information war on the bases of motivation, target, and method (Lachow, 2009:439). The second one deals mainly with the purposes of hacktivism, cyber crime, cyber espionage, cyber sabotage, cyber terror, and cyber war (displayed from the lower to the higher level of potential damage, and from the higher to the lower level of potential probability) (Cavelty, 2012:116).

Both classifications are very abstract and treat the same events with different labels. For Lachow (2009:440) Estonia was just a case of hacktivism, while for Cavelty (2012:109) Estonia should be understood as one of the "main incidents dubbed as cyber war". Why do those differences matter? Mainly because depending on the framing of a problem, the ensuing political responses will vary. The more securitized a social event is, the more exceptional and extreme can be the governmental responses to it (Buzan, Waever, et. al., 1998).

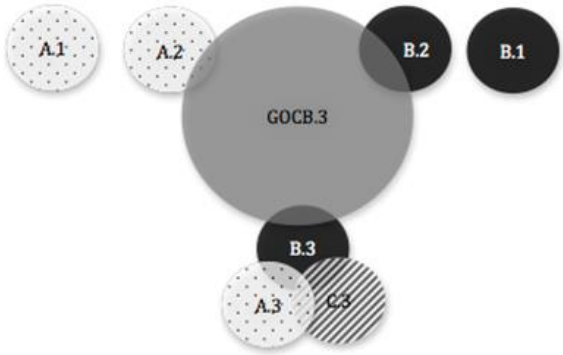
Treating activism, criminal activities, terrorism, and acts of war interchangeably undermines the state capability to adequately respond to a specific threat or conflict. Equally important, by throwing

different categories of actors under the same umbrella, it poses real threats to the civil liberties and political rights of individuals all around the world, despite the type of political regime they live under. For as Betz (2012:694-695) reminds us, cyberspace

> "[…] Extended a number of command, control, communications and intelligence capabilities [to non-state actors] which only the richest states could afford two decades ago; but the best picture is rather different with the state use of cyberspace as a means of war. For one thing, as the Stuxnet virus, which targeted the Iranian nuclear program, demonstrates very well, such capabilities do not come cheap […] For the purposes at hand, however, the significant thing about Stuxnet (which in historical perspective may be seen as the Zeppelin bomber of its day – more important as a harbinger of what is to come than for its material contribution to the conflict at hand) is that it was not the work of hackers alone but of a deep-pocketed team which had both excellent technical skills and high-grade intelligence on the Iranian program."

In sum, asking the right questions while assessing anything "cyber" is thus necessary to avoid either trivializing real wars that might come or undermining civil and political rights when treating all cyber conflicts as war.

Figure 1. Simplified Graphical Representation of Cyberspace



The illustration does not intend to represent the different sizes and individual characteristics of each system. Adapted from Zimet; Barry (2009:288) and Libicki (2012:326).

REFERENCES

Arquilla, J. and D. Ronfeldt (1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: Rand Publishing.

Betz, D. (2012). "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies*, 35:5, 689-711.

Biddle, S. (2012). "LulzSec Leader Betrays All of Anonymous." Gizmodo. http://gizmodo.com/5890825/lulzsec-leader-betrays-all-of-anonymous (accessed August 8, 2014).

Blumenthal, M. and D. Clark (2009). "The Future of the Internet and Cyberpower." In *Cyberpower and National Security*. F. Kramer, S. Starr and L. Wentz. Washington, D.C.: National Defense University Press.

Buzan, B. and O. Waever, et al. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.

Castells, M. (1996). *The Rise of the Network Society*. Oxford: Blackwell.

Castells, M. (1999). *Information Technology, Globalization and Social Development*. Geneva, Switzerland: United Nations Research Institute for Social Development. http://www.unrisd.org/unrisd/website/document.nsf/ab82a6805797760f80256b4f005da1ab/f270e0c066f3de7780256b67005b728c/$file/dp114.pdf (accessed August 8, 2014).

Cavelty, M. D. (2012). "The Militarisation of Cyber Security as a Source of Global Tension." In *Strategic Trends 2012: Key Developments in Global Affairs*. D. Möckly. Zurich: Center for Security Studies (CSS), ETH Zurich. http://www.css.ethz.ch/publications/Strategic_Trends_EN (accessed August 8, 2014).

Childress, J. F. (2001). "The War Metaphor in Public Policy: Some Moral Reflections." In *The Leader's Imperative: Ethics, Integrity, and Responsibility*. J. C. Ficarrota. West Lafayette: Purdue University Press.

Clark, W. K. and P. L. Levin (2009). "Securing the Information Highway: How to Enhance the United States' Electronic Defenses." *Foreign Affairs*, 88:6 (November/December 2009). http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway (accessed March 27, 2015).

Clarke, R. and R. Knake (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco Press.

Clausewitz, Carl von. (2007). *On War*. Oxford: Oxford University Press.

Collier D. and J. Mahon (1993). "Conceptual 'Stretching' Revisited: Adapting Categories in Comparative Analysis." *The American Political Science Review*, 87:4, 845-855.

Colombia.com (2012). "Expertos Creen que Estamos Frente a una Guerra 'Cibernética'." Colombia.com. http://www.colombia.com/tecnologia/actualidad/sdi/31440/expertos-creen-que-estamos-frente-a-una-guerra-cibernetica (accessed August 8, 2014).

Demchak, C. (2012). "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* D. S. Reveron. Washington, D.C.: Georgetown University Press.

Denning, D. E. (2009). "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, 1:1, 6-10.

Echevarria II, A. J. (2007). *Clausewitz and Contemporary War*. Oxford: Oxford University Press.

Eriksson, J. and G. Giacomello (2007). *International Relations and Security in the Digital Age.* New York: Routledge.

Fogarty, K. (2011). "LulzSec vs. Anonymous: Doing Hacktivism Wrong." *IT World*. http://www.itworld.com/security/174917/lulzsec-vs-anonymous-doing-hactivism-wrong (accessed August 8, 2014).

Gray, C. (2013). *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle Barracks, PA: Strategic Studies Institute. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf (accessed March 27. 2015).

Goldsmith, J. (2010). "The New Vulnerability." *The New Republic* (June 24, 2010). http://www.tnr.com/article/books-and-arts/75262/the-new-vulnerability (accessed August 8, 2014).

Hansen, L. and H. Nissenbaum (2009). "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 53, 1155-1175.

Joint Chiefs of Staff (2013). "Cyberspace Operations". Joint Publication 3-12(R). http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. (accessed December 12, 2014).

Kim, D. and M. G. Solomon (2010). *Fundamentals of Information Systems Security*. Burlington: Jones & Bartlett Learning.

Kramer, F. and S. Starr and L. Wentz. (2009). *Cyberpower and National Security*. Washington, D.C.: National Defense University Press.

Kuehl, D. (2009). "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*. F. Kramer, S. Starr and L. Wentz. Washington, D.C.: National Defense University Press.

Kurbalija, J. and E. Gelbstein (2005). *Gobernanza de Internet: Asuntos, Actores y Brechas*. Geneva: Diplo Foundation.

Lachow, I. (2009). "Cyberterrorism: Menace or Myth." In *Cyberpower and National Security*. F. Kramer, S. Starr and L. Wentz. Washington, D.C.: National Defense University Press.

Libicki, M. C. (2012). "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy*, 8:2, 325-340.

Lucas, M. (2012). "Matrix, o el Nuevo Campo de Batalla." *Revista DEF*. http://www.defonline.com.ar/?p=8935 (accessed August 8, 2014).

Lynn, W. F. (2010). "Defending a New Domain: The Pentagon's New Cyberstrategy." *Foreign Affairs* 89:5 (September/October 2010). http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (accessed August 8, 2014).

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Nakashima, E. (2011). "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses." *The Washington Post* (October 17, 2001). http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn (accessed August 8, 2014).

Nissenbaum, H. (2005). "Where Computer Security Meets National Security." *Ethics and Information Technology*, 7, 61-73.

Noro, L. (2012). "Cyber War: La Guerra Silente." *Revista DEF*. http://www.defonline.com.ar/?p=9064 (accessed August 8, 2014).

O'Harrow, R. (2006). *No Place to Hide*. New York: Free Press.

Reed, T. (2005). *At the Abyss: An Insider's History of the Cold War*. New York: Random House Publishing Group.

Rid, T. (2012a). "Cyber War Will Not Take Place." *Journal of Strategic Studies*, 35:1, 5-32.

Rid, T. (2012b). "What War in the Fifth Domain?" Kings of War (9 August, 2012). http://kingsofwar.org.uk/2012/08/what-war-in-the-fifth-domain/ (accessed August 8, 2014).

Rid, T. (2013) *Cyber War Will Not Take Place*. London: Oxford University Press.

Roberts, P. (2012). "LulzSec informant Sabu Rewarded with Six Months Freedom for Helping Feds." Naked Security (August 23, 2012). http://nakedsecurity.sophos.com/2012/08/23/sabu-lulzsec-freedom/ (accessed August 8, 2014).

Sartori, G. (1970). "Concept Misinformation in Comparative Politics." *American Political Science Review*, 64, 1033-1053.

Schmitt, M. N. (1999). "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *The Columbia Journal of Transnational Law*, 37, 885-937.

Sommer, P. and I. Brown (2011). *Reducing Systemic Cybersecurity Risk.* Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3. http://eprints.lse.ac.uk/31964/ (accessed August 8, 2014).

Stamp, M. (2011). *Information Security: Principles and Practices*. Hoboken: Wiley.

The Economist (2010). "War in the Fifth Domain." *The Economist* (July 1, 2010) http://www.economist.com/node/16478792 (accessed August 8, 2014).

USA (2005). "U.S. National Defense Strategy." http://www.defense.gov/news/mar2005/d20050318nds1.pdf (accessed August 8, 2014).

USA (2012). "Sustaining US Global Leadership: Priorities for 21st Century Defense."http://www.defense.gov/news/defense_strategic_guidance.pdf (accessed August 8, 2014).

Uzal, R. (2012). "¿Es la Guerra Cibernética el Desafío más Relevante de la Defensa Nacional?" Mochila Virtual - Infantería Argentina (December 5, 2012). http://www.mochiladelinfante.com.ar/defensa/89-yies-la-guerra-cibernytica-el-desafno-mbs-relevante-de-la-defensa-nacional.html (accessed August 8, 2014).

Van Creveld, M. (2007). "War and Technology." Foreign Policy Research Institute Footnotes, 12:25. http://www.fpri.org/articles/2007/10/war-and-technology (accessed March 27, 2015).

Washington Post (2012). "U.S. Accelerating Cyberweapon Research." *The Washington Post* (March 13, 2012). http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story_1.html (accessed August 8, 2014).

Weimann, G. (2004). *Cyberterrorism: How Real Is the Threat?* Washington, D.C.: United States Institute of Peace. http://www.usip.org/files/resources/sr119.pdf (accessed August 8, 2014).

World Internet Users and Populations (2012). "Internet Usage Statistics – The Internet Big Picture." http://www.internetworldstats.com/stats.htm (accessed August 8, 2014).

Zimet, E. and C. L. Barry (2009). "Military Service Overview." In *Cyberpower and National Security.* F. Kramer, S. Starr, and L. Wentz. Washington, D.C.: National Defense University Press.

Argentina Space: Ready for Launch

Daniel Blinder

Desire for a comprehensive space program, one that includes an indigenous satellite launch capability, motivated Argentina to strengthen relevant policy institutions and carefully reconsider its approach in foreign affairs. In the process, this space power on the semi-periphery bridged bitter domestic partisan differences on the federal budget and allayed security fears of the international community, fulfilling at least some important national objectives regarding economic development as well as Argentinean access to space.

Argentina has pursued space technology development since the 1960's, and this development has always been linked to national political forces.[1] In Arturo Frondizi's presidency (1958-1962) the National Commission on Space Research (CNIE) was created and immediately subordinated under military control. Since then, many remarkable goals were achieved: the rockets Alfa, Beta, and Gamma Centauro; subsequent projects Orion, Castor, Rigel, Tauro; and especially the Canopus II, which launched a monkey into space and brought it back alive.[2]

However, there was no policy aimed at institutionalizing space programs that continued across political administrations, and often there was a fine line between civilian and military activities[3]: This could be explained because no democratic consolidation existed until 1983, and space activities were not consolidated until the 1990's, when a shift of political direction brought more intense and productive linkage between two processes: foreign and space policy.[4] For methodological purposes, space policy is defined broadly in this paper to include all those explicit or non-explicit policies, planned or unplanned, systematically or non-systematically organized, which are aimed toward developing or having space capabilities.[5]

The point of view we take tests a somewhat controversial assumption that different theoretical approaches are needed to understand the international and political environment of peripheral states. What is the real connection between foreign policy and space policy in a middle-income country like Argentina, and our employment of specialized theoretical frameworks like Peripheral Realism or Dependency Theory? The scholar and former advisor to Argentina's foreign minister Carlos Escudé introduced his theory of peripheral realism by trying to understand the world not from the viewpoint of the world powers, but from the countries of the

[1] Dr. Daniel Blinder is researcher at the Centre for Studies on History of Science and Technology, José Babini, National University of San Martín (UNSAM) and professor at the National Defense School (EDENA) in Argentina.

[2] The CNIE achieved technological successes. However, due to traumatic political events in Argentina during the 1960s and 1970s, and the lack of an explicit direction or clear technological development project, CNIE never solidified as an institution. Other issues likely contributed to low institutionalization such as the international context of the Cold War and the influence of that bipolar conflict upon diffusion of technologies on the periphery. In my doctoral research I tracked institutional documents with scarce results: not many documents could be found about CNIE (as would be expected for a politically sensitive and highly personalized organization).

[3] To read more about the ambiguous line between civil and military activities see: J. Johnson-Freese (2007), *Space as a Strategic Asset* (New York: Columbia University Press).

[4] Satellites are another stage of technology policy in Argentina, related to the institutionalization of space policy and the creation of the National Commission on Space Activities (CONAE) under civilian control. Since the 1990's onwards, Argentina has successfully built satellites such as Lusat-1, Victor-1, SAC-A, SAC-B, SAC-C, SAC-D, and SAOCOM.

[5] Launcher, satellite, or both.

periphery.[6] According to Escudé, the international system has an incipient hierarchical structure based on perceived differences between states: those that have power and give orders, those that do not have power and obey, and those that rebel.

His approach introduced a different way to understand the international system: that is, from the unique viewpoint of states that do not impose the rules of the game in the international arena, and which suffer high costs when they confront them. Therefore, foreign policies of peripheral states are framed and implemented in such a way that national interest is defined in terms of development, confrontation with great powers is avoided, and autonomy is not understood as freedom of action but in terms of the costs of using that freedom. Escudé recognized that his theory is indebted to Dependency Theory, which is essentially a theory to explain lack of or perverse development. Notwithstanding, Peripheral Realism is also a "periphery and core" theory, and according to Escudé, many "realists" were actually peripheral realists because they read the international environment realistically and from the periphery: Big powers object, bully, or even destroy small powers when these have the temerity to challenge international written or unwritten rules.[7]

The following sections of this article first analyze ruptures and continuities of domestic politics and foreign policy regarding missiles and space for Argentina during the Menem (1989-1999) and Kirchner/Fernández de Kirchner (2003-2012) presidencies. The article then discusses whether space policy on the periphery is primarily a matter of security or development, taking Argentina as a case study of space technology on the semi-periphery. This paper traces the pathway toward strong institutions regarding space policy and examines the topic of Argentina as a reliable state: a country that conforms to legitimate codes of conduct in world affairs with regard to its space activities.[8] Finally, it argues that institutions matter when a state embarks on development of sensitive dual-use technology. There is a strong relationship between technology acquisition and international relations. Consequently, peripheral states in general, not just Argentina, are more likely to succeed in development and national security aims when they consciously integrate their technology policy with foreign policy.

SECURITY OR DEVELOPMENT?

The foremost institutions that played a role in the consolidation of space policy in Argentina were the Ministerio de Relaciones Exteriores (Ministry of Foreign Affairs), Comercio International y Culto (MRECIC), and CONAE (National Space Commission). The first one depended directly on the president; even so, the political direction was imprinted in MRECIC, and MRECIC is still one of the most professional bureaucracies of Argentina, along with the Armed Forces. CONAE is also a professionalized institution, and until 2012 it was under the MRECIC umbrella. The aim of this institutional hierarchy was to have a dual purpose for space policy. First, space was a venue for foreign policy and the pursuit of peace through carefully calibrated international objectives, nuclear nonproliferation policy, and cooperative Argentine foreign policy on sensitive issues such as technologies related to war. The second purpose of space institutions was to achieve technical objectives such as satellites and launchers.[9]

Considering technology policy as part and parcel of foreign policy, both substantively and institutionally, we can draw lessons for managing

[6] C. Escudé (1992), *Realismo Periférico: Fundamentos para la Nueva Política Exterior Argentina* (Buenos Aires: Planeta).

[7] C. Escudé (2012), *Principios de Realismo Periférico: Una Teoría Argentina u Vigencia ante el Ascenso de China* (Buenos Aires: Lumiere).

[8] My use of the term "reliable" or "reliability" stems from politicians, diplomats, and space policy actors' regular use of this term in Spanish. The word refers to the reliability of behavior for a country, which follows (and is believed to follow) international norms.

[9] On the one hand, space policy was a top-down process in which political leaders used space as a foreign policy issue, and later as a development issue as well. But in CONAE it was not only Conrado Varotto leaving his mark as director. Diplomats, technicians, engineers, mathematicians, physicists, and astronomers became influential, also, in a bottom-up process.

tradeoffs between national security and development objectives. To begin, we try to understand the decision-making processes on research, development, and cancellation of the *Condor II* missile project in Argentina during the 1990s. The *Condor II* project was initiated during the last military dictatorship (1976-1983), and the subsequent (Radical Party) civilian government of Raúl Alfonsín took the political decision to go ahead with it, disposing institutional and economic expenditures for this purpose. Nevertheless, *Condor II* was restricted in practice, and paralyzed later, due to hyperinflation and economic crisis. At the same time, European companies financed the project,[10] linking it to Middle Eastern countries, namely Egypt and Iraq, and changing the focus from an economic development agenda to an international security agenda, given international sensitivity toward those countries suspected of weapons proliferation.

The ending of the *Condor II* project and the emergence of the civilian National Commission on Space Activities (CONAE) were two connected events. Again, before the creation of CONAE, the national space institution was the National Commission on Space Research, under the Air Force, and space policy was not sufficiently institutionalized.

Condor II was a medium-range missile developed in Argentina under Air Force auspices. Its development started between the end of the 1970s and the beginning of 1980. For military aviation, it became a strategic project after Argentina had been defeated in the Falklands War (1982) and the Air Force had lost deterrent capability along with its aircraft and fighter pilots. Though *Condor II* received contributions from both European companies and countries such as Egypt and Iraq, its development was classified.

Due to its secretive nature and the reputation of certain countries supporting its construction, the United States pressured Argentina to deactivate the project for the sake of limiting missile proliferation and stabilizing international security.[11] At the same time Argentina was developing the Condor project, it was developing nuclear technology as well, which was in fact, a part of the strong tradition of this South American country. From the 1960's, in these two sensitive technologies Argentina had important advances, linked always to a nationalist ideology, developmentalism, and the regional security dilemma with Brazil.[12] This explains why military institutions were involved. In Harding's words, "a technological and political maxim that materialized during the space age is that there has been an inexorable and symbiotic relationship between space programs, missile technology, and nuclear programs, whenever technologically and politically feasible".[13]

The foreign policy of President Carlos Menem (1989-1999) radically changed the traditional positions of the Argentine Republic in international relations. In the context of his presidency, the world was also mutating in a

[10] According to the 1985 Secret National Decree, which created the institutional frame for the "Satellite Plan," the name given to the project *Condor II*, and further investigations that linked companies, the contract between the Air Force with Aerospace SA (a company composed by the Argentina Air Force and other small national companies) led to interactions with several European countries. Consen (Consulting Engineers) had by then headquarters in Switzerland and Monte Carlo, and was a subsidiary of the Messerschmitt Bölkow Blohm, Daimler Benz. IFAT Corporation had relations with the Ministry of Defense of Egypt, and Desintec was a West German company. Consen worked with Italian SNIA-BDP, a subsidiary of Fiat, and with the French SAGEM. See D. Blinder (2011), *Tecnología Misilística y Sus Usos Duales: AproximacionesPolíticas entre la Ciencia y las Relaciones Internacionales en el Caso del V2 Alemán y el Cóndor II Argentino*. Revista Iberoamericana de Ciencia Tecnología y Sociedad (CTS), 6 (18): 9-33; see also R. Diamint, "Cambios en la Política de Seguridad. Argentina en la Búsqueda de un Perfil no Conflictivo". N°7, Vol. VII, Chile: Flacso. Both papers summarize links between European companies and the Middle East.

[11] The United States was concerned about *Condor II*'s potential to serve as a Weapon of Mass Destruction (WMD) delivery system.

[12] Emanuel Adler (1987), *The Power of Ideology. The Quest for Technological Autonomy in Argentina and Brazil* (Berkley: University of California Press).

[13] R. Harding (2013) S*pace Policy in Developing Countries: The Search for Security and Development on the Final Frontier* (London: Routledge), p. 16.

radical way: the Soviet Union disappeared, and the tensions of the Cold War faded. The United States emerged as an international superpower, and in that context, Argentina had a long tradition of anti-Americanism in its foreign policy, a tradition that Menem proposed to change, opening up to free trade and generating "special"[14] relations with the major world power.[15] However, the economic, political, and social crises that affected Argentina towards the end of the Menem administration (and that deepened in the following presidency of Fernando de la Rua) resulted eventually in a rupture of national leadership and a major change of direction on political and economic issues with President Kirchner in 2003. Kirchner's administration proposed to restart and develop the industrial policy that had existed before Menem, recover the economy on the basis of import substitution, and project foreign policy especially toward South America. Although there was some confrontation with the United States, institutional frameworks of foreign policy made in the 1990s nevertheless continued, for example, the stable Argentine policy positions on international security and terrorism[16]. But under Menem's administration, technological development was limited while under Kirchner's, the country sought to develop its own technological capabilities, organic to the country's productive means.

The foreign policy objectives of the 1989-1999 period with respect to space policy were "special relations" with the United States and a successful quest for international reliability. Notwithstanding these efforts, results of 'technology policy' from the period, derived in conjunction with the free market economy, were deindustrialization of the country and technological denationalization. In contrast, again, for the period 2003-2012, the foreign policy, in broad terms, resulted in good relations with the United States, cooperation in the major international forums in the field of security, and establishment of a South American orientation. Technology policy of the Kirchners was different in that it was activist and industrialist, promoting national scientific and technological development.

The political role of technology called 'sensitive' in peripheral contexts is a key issue encompassing missile and satellite launcher programs.[17] For developing nations that seek to exploit space technology in general, counting all satellite launchers as sensitive technology is problematic and contentious. On the other hand, having missile launch technology mastered by fast developing nations is also controversial because this has destabilizing effects and poses consequent dangers for world peace and international order. Especially for peripheral countries in the international system, security related to nonproliferation is incompatible with the right to development, that is, of non-central countries to develop new technologies for export-led growth.

In this environment, *Condor II* and CONAE[18] were salient cases for institutionalization of a technology policy, linking it directly with foreign policy. The Condor missile was a defense project begun during the military dictatorship in Argentina. The ultimate destruction of this missile and abandonment of the program was the reason for creating CONAE. The new Argentine space agency was institutionalized through bilateral relations with other space agencies as an insurance policy. This way, Argentina would only develop space technologies for peaceful purposes consistent with the standards of multilateral regimes such as the Missile Technology Control Regime (MTCR), the UN Committee on the Peaceful Uses of Outer Space (COPUOS), etc.

[14] C. Escudé (1992) *Realismo Periférico: Fundamentos para la Nueva Política Exterior de Argentina* (Buenos Aires: Planeta).

[15] F. Corigliano (2003), "La Dimensión Bilateral de las Relaciones entre Argentina y Estados Unidos durante la Década de 1990: El ingreso al Paradigma de las 'Relaciones Especiales'," en Carlos Escudé (Ed.), *Historia General de las Relaciones Exteriores de la República Argentina*, Parte IV, Tomo XV (Buenos Aires: GEL).

[16] C. Escudé (2012), *Principles of Peripheral Realism* (Buenos Aires: Lumiere).

[17] Countries that have the capability to launch satellites are the United States, France, Japan, China, Great Britain, the European Space Agency, India, Israel, Ukraine, Russia, Iran, and North Korea.

[18] National Commission on Space Activities, again, the space agency of Argentina.

What drove Argentina toward a dramatic institutional change in order to pursue similar space launch technologies? Recall that *Condor II* affected military interests because it (a) could be a military threat to future targets of the Argentine state (the Falklands/Malvinas War was close in time); and (b) could be sold to other nation-states, which would use it for military purposes. Yet, *Condor II* also affected commercial interests due to the fact that (a) the missile system included dual-use technology, and, as the military technology was also part of international trade, missile technology suppliers feared market competition; and in addition (b) the missile technology could be used for space exploration and to orbit satellites for commercial reasons.

ARGENTINA AS A CASE STUDY OF SPACE TECHNOLOGY ON THE SEMI-PERIPHERY

Studying the case of space policy in Argentina allows us to make some informed conjectures on the role of peripheral states in the development of sensitive technology projects. Specifically, space technology on the periphery brings out the relationship between domestic policy and technology policy in developing countries, and some tensions between the sovereign right to development and security limits imposed by the international order. Does every country have the right to develop dual-use technologies that only a select club of space powers currently possesses?[19] In the case of Argentina, a semi-peripheral state, there are direct and indirect pressures from central states of the international system, threats of sanctions or other impediments, aiming to prevent access to sensitive technologies, treating them as weapons of war.[20]

Despite major changes in political orientation, there was institutional continuity between 1989 and 2012. Cancellation of the Condor project, signing and ratification of nonproliferation treaties, confidence-building measures toward the United States, and neoliberal[21] economic policies implemented in the first period (1989-1999) had a decisive impact on the second period (2003-2012). However, the success of the second period corresponds with economic policies (Keynesianism or state intervention; industrialization; and foreign policy focusing on regional integration, especially Latin America) in opposition to those of the first. The institutional consolidation of CONAE and intervention of the Foreign Ministry, cooperating in all these matters with the United States (enduring agreements with NASA, ratification of nonproliferation treaties), marked the course of development of space technology for the next decade. Numerous ongoing satellite missions, today, and the development of a satellite launcher, the Tronador II,[22] are products of successful institutions, as opposed to specific political parties or private sector corporations, guiding technological development.

Journey toward Strong Institutions

Condor II and the military dictatorship, 1976-1983: The reasons for the Argentine military to protect *Condor II* contemplated geopolitical and economic considerations and a vision for the country to become a technological powerhouse, to increase its military power after defeat in the Malvinas War. With this goal in mind, the

[19] See R. Harding (2013), S*pace Policy in Developing Countries: The search for Security and Development on the Final Frontier* (London: Routledge). About dual-use technologies this book says that "Besides the bipolar nature of the East–West conflict during the Cold War, one of the traditional constraints on the space programs in developing countries has been restrictions placed on the export of space-related technology. Before 1992, all US satellite-related technologies were classified as "munitions" and therefore subject to regulation by the US State Department under a regime known as the International Traffic in Arms Regulations (ITAR). During the mid-1990s, these restrictions were eased for "dual-use" technologies, which are those not exclusively military in purpose and application. The line between the two concepts in practice, however, is nebulous, since essentially all space technology is dual-use."

[20] By semi-periphery, we mean a country on the periphery of the international system but which has some kind of industrial and technological development,

[21] Free market economy, market deregulation, no State intervention, and privatization.

[22] Having a national launcher is considered by the space authorities in Argentina as a goal for autonomous technological development in space.

military, without any public oversight,[23] did not behave as a responsible social group in terms of technology management. But the context is relevant, here: The Condor project was the fruit of a military dictatorship in which the Air Force was a political player of the first order. As such, and bereft of any control, they did what they wanted to do. In the follow-on civilian administration of President Alfonsín, the military were no longer the political power, but the power of the military lobby was still strong. In that sense, during the period of the return to democracy, the government of Alfonsin could not be characterized as free from pressures of the "military party" and, for that reason, Condor remained unaccountable to the Argentine public.

Condor II and the Alfonsín Government, 1983-1989: During the administration of Raul Alfonsín, *Condor II* took on greater dimensions, expanding its financing through capital from Middle Eastern countries—Egypt and Iraq—as well as funds from domestic and European companies, through a secret presidential law.[24] Even so, the project was halted due to the lack of a budget: There was always difficulty assessing the true financial costs of *Condor II* and political irresponsibility when it came to promoting missile development incompatible with the economic and financial circumstances of the country. Argentina was undergoing major economic and monetary crises caused by high, uncontrolled inflation. There were informal pressures during this period. Defense officials received through several channels messages from the American government linked to the missile project and concern over its eventual use. During the subsequent Menem government, Argentina did enter the Missile Technology Control Regime (MTCR), a decision arising from international pressure as well as Menem's pro-American instincts.

Condor II and the Menem Government, 1989-1999: During the Menem government, the Condor missile came to light, taking on status as a public issue. In addition, the international context transformed. The Soviet Union imploded, and the United States was emerging as the single superpower. In Menem's presidential term, international pressure for cancellation and destruction of Condor could no longer be denied in political discourse. The missile became an irritant in bilateral relations with the United States. With Argentina's new foreign policy of alignment and the urgent need of international credit for managing the country's external debt, Menem decided to terminate it. The creation of CONAE under the Ministry of Foreign Affairs was the plan adopted by the Menem government, aiming to institutionalize pillars of foreign affairs and space issues.[25] Due to this same impulse, the government signed international security treaties such as the MTCR. Agreements were also signed with NASA, and joint satellites were developed and launched. But an indigenous launcher was not considered, given the bilateral conflicts that had emerged over *Condor II*. Instead of investing enormous quantities of money to make a launcher that would arouse international suspicion, launch services were hired when needed.

Success or Failure?

Was Argentina's foreign policy between 1989 and 2012 regarding space policy a success? Destroying the Condor missile and creating CONAE was a long-term policy. Could it be assessed as positive? Broadly speaking, the government of Menem de-industrialized the economy, binding decisions of technology policy to "market forces." Neoliberalism and special relations with the United States were two facets of this policy agenda. By the same token, special relations with the United States led Argentina to higher status in terms of international trust and access to technologies that before were denied due to an erratic policy on space. The Menem administration complemented strategic agreements with NASA with policies that aimed to build a good relationship with the American

[23] The govermment was a dictatorship; no checks and balances existed as in a pluralistic democracy in which the budget and infrastructure projects are public domain and under control of democratic institutions.

[24] A Secret and Executive Order under the law of Argentina of 1985, quoted above.

[25] F. Corigliano (2003), "La Dimensión Bilateral de las Relaciones entre Argentina y Estados Unidos durante la Década de 1990: El Ingreso al Paradigma de las 'Relaciones Especiales'," en Carlos Escudé (Ed.), *Historia General de las Relaciones Exteriores de la República Argentina*, Parte IV, Tomo XV (Buenos Aires: GEL).

government as a whole. Argentine-U.S. space cooperation included the launching of *μSAT-1*, the experimental satellite *Victor* in 1996, the *SAC-B* in 1996 to study the sun, the *Nahuel-1A* in 1997, the *SAC-A* in 1998 with experimental objectives, and the *SAC-C* in 2000 for earth observation. All these satellites were launched by rockets from other countries, of course. They were meant to send a clear signal to the United States that Argentina would not develop its own ballistic missile. Nevertheless, due to solid space institutions under CONAE, Argentina advanced its national space capacities and achieved international recognition.

Since the creation of CONAE, institutional foreign policy has borne fruit: If we compare technological achievements from before and after creation of the agency, CONAE is clearly associated with new space capacities. Had Argentina remained burdened with the Condor missile project,[26] it is unlikely the country could have pulled off this performance. Technological outcomes were also tied to industrial policy started in 2003 by the Kirchner administration. The need for a public policy on industrial and technological development tied to a responsible foreign policy is indicated. All these policies were important elements of a grand strategy built around national development.

INSTITUTIONAL CONTINUITIES MATTERED MORE THAN POLITICAL RUPTURES

Discontinuities in the 2003-2012 period: A new non-confrontational foreign policy toward the United States, active participation in the MTCR (and other agreements such as non-proliferation treaties), cooperation with NASA and other agencies, and of course, the process of institutionalization of the space sector focused on CONAE, against these endeavors, we can question, what were key discontinuities in the 2003-2012 period? First, the country changed from a non-industrial economic model in the 1990s, to a model of industrialization in the Kirchner presidency. In terms of technology development, there was a greater emphasis on multilateral foreign policy, especially toward South America, the ongoing development of a domestic launcher (Tronador), and a sequence of Argentine satellites placed into orbit. For Argentina, development of a rocket engine or a communications satellite was no longer wedded to a nonnegotiable national security strategy of nuclear deterrence. On the other hand, national prestige and compensation for wounded pride of the military defeat in the Malvinas War were only feasible through civilian-run programs at CONAE, and left-of-center governments in the post-Menem era wisely appreciated both enduring political objectives.

International Reliability

The issue of Argentina's climb to respectability as a powerful partner in Latin America also relates to the shift from a secret space program under the military dictatorship to open institutionalization under CONAE. Prior to that change, Argentina had confrontational discourses and policies, and was reluctant to follow U.S. international leadership. The American diplomatic response included a storyline that continued over many years, consisting of diplomatic efforts (formal and informal) to paint the South American country as a state that promoted proliferation, a U.S. narrative that gained credence from Argentina's historical attempts, under military leadership, to develop space and nuclear technologies.

The way it was imagined internationally, Argentina was not reliable during the dictatorship because it was a military government that seized power, menacing neighbors and killing its own people without trying them in a legal court. After that, even with the democratic government of Alfonsín, Argentina was not reliable because it was a weak and incipient democracy—army attacks against the government in order to return to military rule had already taken place. Then, in the days before the inauguration of Menem, Argentina was not reliable because it was going to be ruled by a nationalist and xenophobic government, rooted in Peronist doctrine. Such a doctrine had frequently been associated with confrontational behavior towards the United States. In the end, even with the Menem

[26] The Condor project lacked an institutional frame, on-budget investment, and a compatible, supportive foreign policy.

government showing clear signs of alignment with the West on foreign policy, it was required by the H.W. Bush administration that the *Condor II* missile be destroyed. This was accomplished under Menem, though much later, during Kirchner's administration, alarms still dogged the claim that Argentina yearned for an indigenous satellite launcher.[27]

When Argentina's past unreliability was mentioned within the international community, what was being transmitted was a representation built by U.S. diplomacy, the mass media, and the universities.[28] The categorization of reliability was divorced from actual threats to the national security of the United States, to international peace, and to non-proliferation of weapons of mass destruction. Rather, the epithet was married to political economy, to political and economic gambits, the main objective of which was economic and military supremacy of the hegemonic power. The pursuit and continuance of hegemony along key dimensions of international power still involves control of sensitive technologies, which really do pose danger to U.S. dominance if they spread around the world.

This leads us to think about arguments couched in security terms that mask commercial interests. Such arguments are not necessarily conspiratorial. Whether the space technology in question is domestic or foreign, a country that wants to have some place among nations, "a place in the sun," and that wants to improve its citizens' standard of living would use state of the art technologies: Rockets and satellites are among them. Without using space technology, a country, in general, loses in the field of economic development. Using alien and so-called reliable technology, though, often marks a path to dependency. From an analytical point of view, it is impossible to separate concepts of safety and business. How far does commercial interest extend until political interest or security reasons, not related to commercial ones, compel a central power to impose technological bans or restrictions on peripheral countries? A sensitive technology has always both sides of the coin, and a peripheral country who does not write the rules of the game is in a disadvantaged position in comparison with a central state who does write such rules.

A quick glance shows that countries with reliable space technology are the United States (major world power), Russia (former Soviet Union and previous world power), France (and through it the European Space Agency), Japan, China, India, Israel, Ukraine, and South Korea. Countries with unreliable space technology are Iran and North Korea. Again, what makes some reliable and not others? Which category will describe countries such as Argentina or Brazil that develop in the next decade satellite launchers? Without predicting precisely what will happen in technology development, acceptance of Argentina as a space power will depend upon written and unwritten international rules as well as the interests of the U.S. hegemon. Should the current trend toward multipolarity deepen, wise and moderate diplomacy from Argentina and other semi-peripheral states could raise the chances of these countries achieving reputation and *de facto* legitimation as reliable space powers, with all the attendant commercial and security benefits.[29]

Years after the consolidation of space policy at CONAE, Argentina developed the GRADICOM[30] missile project, which raised concerns on external and internal levels, including diplomatic officials and CONAE members, who wanted to be explicitly separated from any activity qualified as

[27] *La Nación*, 24/04/2011. "EEUU Terminó un Plan para Revivir el Misil Cóndor."

[28] D. Hurtado de Mendoza (2010), *La Ciencia Argentina. Un Proyecto Inconcluso. 1930-2000* (Buenos Aires: Edhasa).

[29] Written and unwritten rules include the claims upon the Falkland/Malvinas Islands in the United Nations and in other international forums, the repudiation of a war, as such, that drove the military coup, and criticism aimed at nuclearization of the South Atlantic by the United Kingdom (the British are supposed to have nuclear weapons in the Falklands, going against all peace treaties of the regional states). Agreements and treaties attach direct consequences to the status of being a "reliable country" internationally. No such treaty surpasses in importance the Treaty of Tlatelolco for the Proscription of Nuclear Weapons in Latin America and the Caribbean.

[30] Gradicom missile development involves a solid-fuel rocket developed by the Argentine Ministry of Defense for weapons purposes.

military.[31] Despite international pressures, formal and informal, mimicking those that buffeted Argentina in the nineties with respect to the Condor project, GRADICOM may survive in the new international environment. States contending for power on the international scene such as China and Russia now open a horizon of possibilities for Argentina. The strategic alliance with Brazil and MERCOSUR's importance in foreign policy, along with UNASUR and CELAC,[32] indicate a substantial change in the international arena, which reduces priority of relations with the leading powers and lends momentum to the integration and development of other nations. This shift in permissible initiatives, including GRADICOM, presents a window of opportunity in Argentina's case to develop the space sector without crashing directly into the United States or oncoming countries seeking to revise American hegemony[33].

The creation of the Ministry of Science, Technology and Productive Innovation at the end of 2007 changed expectations and linked commercial and security policies even more closely. The system of science and technology must now provide knowledge to increase value-added exports. National industrial recovery requires closure of the technological gap and invites the State, once again, to take an active role in development.

Investment and Technological Development

With the creation and consolidation of CONAE in the 1990s, progress was made in institutional issues, as well as in some access to sensitive technology. Difficult budget decisions notwithstanding, since 2004 annual funding increased as befitting CONAE's strategic status, this despite the new industrial direction of the country under the Kirchners. A glance at Law 24,061 of 1991, which contained the national budget with the newly created CONAE, reveals the amount was 1,587,124,000 pesos for Culture and Education, and for Science and Technology 466,094,000 pesos[34] (Budget 1991).[35] Working from this baseline, the specific budget, in pesos, for CONAE in 2001 was 15,007,037 (Budget 2001), and in consecutive years was 13,896,000 (Budget 2002), 17,023,066[36] (Budget 2003), 13,663,051 (Budget 2004), 39,922,336 (Budget 2005), 73,370,035 (Budget 2006), 120,368,547 (Budget 2007), 203,909,252 (Budget 2008), 293,317,858 (Budget 2009), 260,913,712 (Budget 2010), 346,321,636 (Budget 2011), and 565,174,968 (Budget 2012).[37] The CONAE

[31] Gradicom stirred debates within political and business circles linked to Argentine space policy regarding proliferation. Argentina already has a liquid-fueled rocket for peaceful purposes, the Tronador. Gradicom opened discussion about how a solid-fueled companion would affect civil space, which depends heavily on international cooperation, Argentina's standing in the policy arena of non-proliferation, and foreign affairs, especially those related to conventions in the field of space development.

[32] MERCOSUR (Southern Cone Common Market) includes Argentina, Brazil, Uruguay, Paraguay, and recently Venezuela. It is an alliance of free trade and the axis of integration between Argentina and Brazil since the 1990s. UNASUR (South American Union of Nations) is an Alliance of countries in the territory of South America, whose diplomatic objective is to achieve regional integration. CELAC (Community of Latin American and Caribbean States) is a diplomatic alliance with objectives of integrating nearly all countries of the Western Hemisphere. Successor to the Rio Group, it is an institutional alternative to the Organization of American States, which includes the United States.

[33] Further evidence of informal pressure on Argentina was the broadcast concern of CONAE Administrator Conrado Varotto to be reliable to the United States and show that space development in Argentina was peaceful at all aspects.

[34] From 1991 to 2002, established by the "Convertibilidad" Law, 1 peso was equivalent to 1 U.S dólar.

[35] Until 2001, the budget is hard to find published or online. To take an example, the budget of 1991 was not only obscure with respect to space technology; it did not specify expenses by item, which makes it nearly impossible to classify where the money went according to law.

[36] From 2003 on, each U.S. dollar was 3 pesos. From 2010 to 2012, each U.S. dollar was 4 pesos.

[37] Presupuesto del Sector Público Nacional de la República Argentina, año 1991. Presupuesto Consolidado del Sector Público Nacional 2001 de la República Argentina. Aprobado por la Decisión Administrativa N°53 del 2 de Mayo de 2001. Presupuesto Consolidado del Sector Público Nacional 2002 de la República Argentina. Aprobado por la

numbers tell a clear tale; they show the growth of the budget during the presidencies of Kirchner and Fernández de Kirchner, exhibiting strong interest in space activity despite their skepticism toward free-market policies. The Kirchners built upon the institutional base of the former Menem period (the 1990s) and supported economic and political sacrifices as technology investments, in terms of budget implementation in space.

To fully appreciate the determination behind this national effort to become a space power, it serves to recall major changes in the international environment coinciding with the domestic transition from Menem to the Kirchners. First, prior to the assumption of Nestor Kirchner, the attacks of September 11 abruptly shifted American policy, which became consumed by war in Afghanistan and Iraq and often neglected South America. Second, the free-market economic policies of Argentina by 2002 led to yet another economic crisis and default. In the context of the new international environment based on regionalism and integration of South America, Argentina found its strongest allies, not within the traditional scope of Europeans, Americans, and Asians, but among its geographical neighbors, progressing at long last along the historical ambition of Latin Americanism in foreign policy.

The Kirchner and Fernández de Kirchner administrations inherited from the Menem presidency, on the one hand, an economic crisis tied to liberal economic measures, but, on the other, a legacy of liberal-oriented international commitments such as MTCR, the Tlatelolco Treaty, and the CONAE space agency with prestigious international ties.[38] Without resources, of course, without a plan for technological development, it is not possible to produce a sensitive technology of strategic importance. But to develop such a technology, a state must also account for strategic behavior of powers in the international system: From 2003 Argentina, under a statist administration that could easily have undercut the national venture in space technology, instead increased significantly the public capital put toward science and technology, and undertook the strategic diplomacy necessary to protect the space sector. The result is observable progress on the satellite launcher, Tronador II, centerpiece of a longstanding national dream to possess an Argentine launcher and blossom on the international stage as a true space power.[39]

Decisión Administrativa N°16 del 18 de Julio de 2002. Presupuesto Consolidado del Sector Público Nacional 2003 de la República Argentina. Aprobado por la Decisión Administrativa N°53 del 19 de Mayo de 2003. Presupuesto Consolidado del Sector Público Nacional 2004 de la República Argentina. Aprobado por la Decisión Administrativa N°134 del 20 de Abril de 2004. Presupuesto Consolidado del Sector Público Nacional 2005 de la República Argentina. Aprobado por la Decisión Administrativa N°257 del 30 de Mayo de 2005. Presupuesto Consolidado del Sector Público Nacional 2006 de la República Argentina. Aprobado por la Decisión Administrativa N°621 del 12 de Septiembre de 2006. Presupuesto Consolidado del Sector Público Nacional 2007 de la República Argentina. Aprobado por la Decisión Administrativa N°243 del 29 de Junio de 2007. Presupuesto Consolidado del Sector Público Nacional 2008 de la República Argentina. Aprobado por la Decisión Administrativa N°154 del 15 de Abril de 2008. Presupuesto Consolidado del Sector Público Nacional 2009 de la República Argentina. Aprobado por la Decisión Administrativa N°339 del 28 de Septiembre de 2009. Presupuesto Consolidado del Sector Público Nacional 2010 de la República Argentina. Aprobado por la Decisión Administrativa N°388 del 7 de Junio de 2010. Presupuesto Consolidado del Sector Público Nacional 2011 de la República Argentina. Aprobado por la Decisión Administrativa N°67 del 30 de Diciembre de 2011. Presupuesto Consolidado del Sector Público Nacional 2012 de la República Argentina. Aprobado por la Decisión Administrativa N°428 del 29 de Junio de 2012.

[38] Liberal as an economic concept means free-market oriented policies and deregulation. Liberal as an International Relations Theory relates to one of the most important schools of thought, focusing on international institutions and cooperation.

[39] The VEX-1A and VEX-1B were test rockets for Tronador II development. Both tests were made in 2014. The first could not fly, but the second was a successful launch.

RECOMMENDATIONS

In countries with weak processes of development and, therefore, without the economic capacity, governments struggle to gain international legitimacy for the use of sensitive technologies. To be a reliable space power, for example, Argentina must not only establish a technically credible satellite vector, it must also demonstrate political and economic capacities to legitimize possession and use of these technologies. If satellite technologies can be considered indispensable in the path toward 21st century economic development, then political unreliability in the fields of proliferation and security becomes a significant obstacle to economic growth[40].

Developing countries such as Argentina should articulate technology policy and foreign policy in such a way that they are really one integrated program for development and diplomacy. For example, if Argentina were to successfully develop a domestic satellite launcher in the coming years, it would come about five decades since world powers were able to produce the first launchers, enough time for this technology to mature.[41] Half a century ago, the race for a satellite launcher meant for Argentina a race to be part of the first group of countries in the 1960s with access to space. In the 2010s, however, launcher technology is becoming less provocative for powers that, years before, developed it. For semi-peripheral states, of course, the technology remains a factor of economic dynamism, and thus a strategic achievement in terms of regional leadership and national prestige.[42]

The unwritten law of the free market requires each independent actor to balance costs and benefits. Consequently, if for Argentina it was more profitable to deliver its own satellites using a *foreign* launcher, this would make investments in local research and development less attractive. Under this free market view, when it was cheaper not to develop the technology, the domestic launcher became unnecessary for the country. Other budget priorities like food, infrastructure, or police filled the vacuum.

Saying that the Condor missile/launcher project, “was no longer necessary for the country" was an affirmation, which at its root denied the value of technology policy. Unfortunately, as we have implied, technology development (even more since the Washington Consensus of the 1990s) is central to any semi-peripheral state with the requisite human capital: for international prestige; regional and global leadership; deterrent capability; expanding markets and new businesses; and creating spillover that accelerates economic development.[43] As the second in command at the Ministry of Foreign Affairs during the Menem administration explained,

"Do you think Argentina can spend five thousand million dollars to put a vector in the air? Brazilians could not. They were not able and they have a budget ten times higher than our own. From fifteen years now they have wanted to put a satellite with a national launcher […] and they couldn't. It is very difficult and very expensive technology. Then, what did the Menem administration do? We could not produce vectors because we were not reliable; the world was going to believe that we were manufacturing costumed missiles. […]. Then, if you want to put a satellite in the sky, you have to go elsewhere, and do what is called the taxi service, hiring the services of countries such as the United States, Europe, China, and Russia. You could hire their services, and you would be putting the satellite in the sky! […] It is

[40] Sensitive technologies are a red line in the overlapping fields of technological capabilities, international politics, and ethics. Hegemonic powers, in order to preserve the status quo, commonly relegate non-core countries to the technological margins, far away from sensitive capabilities and, not incidentally, to economic dependence on lead powers that created and control the contemporary order.

[41] Vernon Ruttan (2006), *Is War Necessary for Economic Growth? Military Procurement and Technology Development* (Oxford: Oxford University Press).

[42] The question of mature technologies is an important issue: "As a field of commercial technology that initially drew heavily on military R&D or military and defense-related procurement matures, its dependence on military and defense-related sources tends to decline. The flow of knowledge and technology may then reverse— from spin-off to spin-on" (Ruttan, 2006).

[43] Ruttan, (2006).

much cheaper to travel by taxi than to buy a car. The most expensive part is not the launch, but the research to achieve it".[44]

Space technology policy in the presidency of Carlos Menem was not focused on research and strategic development but on the laws of the free market and the institutionalization required to gain reliability. The space policy was an excellent institutional policy and a wise foreign policy. But it definitely was not technology policy. The Minister's taxi metaphor spoke to the fact that—in the short term—it is considerably less expensive to hire the launcher than to develop a domestic one. Paying for a car, or pursuing a rocket launcher, results in the domestic capabilities to reach national space goals, but a state must invest a large amount up front: It is necessary to perform the research. Taking a taxi, or renting a launch service, also allows a country to reach space goals, probably faster, but a developing country renting a ride will always be dependent on someone else's car.[45] The choice to have a technology or not, for a country on the semi-periphery, is just as strategic as it would be for an economic and military powerhouse like Russia or the United States.

CONCLUSION

This paper does not endorse building a launcher without analyzing the economic cost of such an effort. On the contrary, having a launcher gives not only greater political autonomy for activities in space but also opens opportunities for economic development: Countries that once struggled to build launchers now offer launching services in the marketplace. The question is why when some countries develop technologies they are innovative while others are rogues that proliferate. The answer is a construction of scholars, media, and diplomacy. While empirical evidence about Argentinean proliferation does not exist, the facts instead show how journalists, politicians, and scholars speculate on the potential and possibilities of such nefarious enterprise. These ideational constructions matter. Regardless of how compliant Argentina is empirically, an international belief that the government is a scofflaw hurts Argentina's national interest: Following Escudé, small powers cannot throw themselves against large powers—even in popular misconception—without paying a real world price.

The ongoing story of Tronador II has highlighted dynamics between international politics and the development of dual-use technologies in semi-peripheral contexts. There is, in fact, a strong relationship between international policy and technological development, no less so on the semi-periphery, where developing countries with great promise face limits or outright bans on technologies already produced and in some cases commercialized by world powers. In addition, powerful states that created the current world order also set the rules of that order. In consequence, written and unwritten laws of the international system determine which countries register as developing a benign space rocket and which others end up ostracized for proliferating ballistic missiles. Despite the serious potential for hostile reactions, semi-peripheral countries that want to grow economically will need to act firmly in their development aims, even as they pay respect to rules of world powers. Under this tension between development goals and cooperation with the international community, technology policy with the proper institutional basis, accommodating to domestic political

[44] Cisneros, Andrés (Vice Canciller). Buenos Aires, May 18, 2010. Interviewed by Daniel Blinder. Quoted from "Globalization, Geopolitics and Sensitive Technologies in Peripheral Situation: Missile/Space Technology in Argentina (1989-2012)." [Globalización, Geopolítica, y Tecnologías Sensibles en Situación Periférica: Tecnología Misilística/Espacial en la Argentina (1989 -2012). Tesis para optar al título de Doctor en Ciencias Sociales por la Facultad de Ciencias Sociales de la Universidad de Buenos Aires.]

[45] This was Varotto's idea, and he explained it, off the record. He went through a litany of reasons why Argentina would not be able to continue relying on the United States or others to get its satellites into space: the high launch costs of acceptable providers and the GOA's unwillingness to run afoul of International Traffic in Arms Regulations (ITAR) by dealing with lower-cost providers of launch services such as China or India. Developing its own SLV (satellite launch vehicle) capability was the least costly alternative for Argentina's space program with such constraints (no documentation/citation available).

constraints of a vibrant democracy, can still flourish.

What are the political and economic benefits of space and other state-of-the-art technologies in the context of semi-peripheral countries? State-of-the art technology gives semi-peripheral countries recognition and extra chips for international negotiation with rule-making world powers. On the economic front, such technology stimulates research and development, technology transfer, and spillover into other areas of international commerce. The story of Tronador II demonstrates that a semi-peripheral country like Argentina can thread the needle in order to reap both diplomatic and developmental benefits from state-of-the-art technology.

The missile/space policy of the Menem government (1989-1999) was to cancel the military's Condor project and bind Argentina through international agreement to nonproliferation as a means of improving relations with the United States. These radical course corrections coincided with institutionalization of space policy, creating CONAE under civilian control with civilian purposes only.

CONAE's careful correspondence with Argentina's broader foreign policy objectives was a key accomplishment of Menem's administration. CONAE's purpose was to pave the road to space for Argentina, in part by facilitating international agreements with foreign space agencies and international treaties. Interestingly, CONAE helped Argentina build its reputation for international reliability during this initial phase without significant investments in launcher technology or groundbreaking satellite projects. Nevertheless, institutionalization through CONAE and a foreign policy of international engagement set the basis for future events of Argentine technological development.

Institutionalization at both domestic and international levels had important consequences during the subsequent Kirchner and Fernández de Kirchner administrations. The institutional frame of CONAE and the main accords of the prior administration under international agencies like the UN and the MTCR continued, actually thrived, as state spending on technology, including space technology, mounted without setting off international alarm bells. With an active policy on re-industrialization and development of science and technology, Argentina achieved its objectives of having satellites in space, and several milestones toward the manufacture of Condor's descendant, Tronador II.

Today, Argentina, against long odds at the cancellation of Condor, is fast becoming a space power, with the capacity to produce satellites and launchers, in cooperation with other countries and while enhancing its reputation for international reliability. Indeed, wise technology policy is more likely to emerge on the semi-periphery in general when public institutions shape it in conformance with enduring goals of *both* strategic diplomacy and national development.

Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?

Nathaniel Youd

2014 Gen. Larry D. Welch Writing Award, USSTRATCOM, Junior Division

After reconsidering massive retaliation versus escalation dominance concepts from nuclear deterrence, escalation dominance, investing in capability to respond proportionally at each level of cyber attack, may be the most practical and effective military strategy for strengthening cyber deterrence.

The past several decades have revolutionized the way we communicate and how modern states wage war.[1] Today it is nearly impossible for most people around the world to go more than a few minutes without their lives being directly impacted by technology and information systems. From the moment a person wakes up to a digital alarm clock, turns on the news and coffee, and takes a shower, every aspect of their lives relies on technology in some way. The growth of the Internet of Things in the coming years will only increase the impact of technology on all aspects of daily life. The information technology revolution has not only influenced the lives of consumers and corporate America but has revolutionized the way wars are fought. The era of the general on the battlefield or the admiral at sea disconnected from higher leadership is gone.

Today a general is more likely to direct the war effort from an operations center surrounded by hundreds if not thousands of digital information streams, from satellite imagery, UAV footage, and information about every troop's digital location, down to real-time audio and video from individual soldiers on the battlefield. While this revolution in military affairs (RMA) and the strategic advantages it gives modern militaries is still fiercely debated, there is little doubt that it has a profound impact on the lethality of modern armed forces and their ability to conduct operations around the globe.

While the technological revolution has shaped modern life and war fighting, it has also created new vulnerabilities that did not exist in earlier conflicts. Although there is still a diverse academic debate about the potential impact and scope of cyber warfare, there is general agreement that a successful attack on information technology systems would have a profound effect on modern social, economic, and military capabilities. In 2012, Secretary of Defense Leon Panetta echoed the warning of several national security scholars when he suggested that a digital "Pearl Harbor" could serve as a wake-up call to the threats of cyberspace.[2]

It is difficult to quantify and evaluate the potential consequences large-scale cyber attacks could have on a modern state, but there is a growing consensus that such attacks would have a profound impact on daily life and severely limit modern war fighting capability. Academics, policy makers, and strategists agree that future wars will not be limited to conventional or nuclear forces but differ in their analyses of the effect cyber threats will have on information technology systems, as well as the appropriate tactical and strategic responses to mitigate such threats. Regardless of who is right, states must begin to adopt policies and strategies for dealing with cyber threats and even deterring aggression in cyberspace. One of the pressing questions in cyber strategy is how to effectively implement a deterrence strategy in the cyber domain. This paper will explore the practicality of cyber

[1] Nathaniel Youd, USAFA Class of '13, is a First Lieutenant in the United States Air Force and a recent graduate of the Columbia University School of International and Public Affairs. The views expressed here are his own.

[2] Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, Department of Defense Press Release, October 11, 2012.

deterrence and will focus on applying traditional deterrence concepts to the cyber domain.

The concept of cyber deterrence is based on the idea that a state or non-state actor can deter a cyber-attack through conventional or non-conventional means, whether through defensive measures, the threat of cyber counterattack, or the potential threat and use of conventional or even nuclear forces. Cyber deterrence is mostly based on prior theories of nuclear and conventional deterrence but faces unique challenges due to the unconventional nature of the cyber domain. The main challenges with cyber deterrence and the academic arguments posed focus on whether or not cyber deterrence should center on retaliation or prevention; the problems that exist with attribution; the debate about rational or proportional response; and the implications of conflict escalation from cyberspace to conventional conflict domains. Each of these issues presents unique challenges for dealing with cyber deterrence and implementing a capable, communicable, and credible cyber deterrence strategy.

DETERRENCE THEORY

In order to understand the applications of deterrence in the cyber domain, it is important to first understand the main concepts behind deterrence theory. These concepts, although most successfully applied to the use of nuclear weapons, have been debated for centuries and can be applicable to all war fighting domains and types. Clausewitz characterized all warfare as "politics by other means,"[3] and Sun-Tzu claimed "the supreme art of war is to subdue the enemy without fighting."[4] While these classical war theorists wrote long before the advent of modern information technology systems or nuclear weapons, their ideas directly apply to deterrence theory.

The essence of deterrence is to raise the cost of fighting in order to "subdue the enemy without fighting." Thomas Schelling's seminal work on deterrence theory, *Arms and Influence*, summarized the core elements of deterrence by claiming that the power to hurt is bargaining power. These two elements – the power to hurt, and the power to bargain – can be applied to any conflict and are the basis of any successful deterrence strategy.[5] Without either element, deterrence strategies cannot succeed.

The key strategies, requirements, and challenges were summarized and applied to cyberspace by Kenneth Geers in his 2010 article in *Computer Law and Security Review*. Geers argues that there are two ways to approach deterrence: one is denial, or the ability to prevent a potential adversary from obtaining capabilities, a more defensive strategy; the other is punishment, or the ability to make the consequences of a certain action so costly that the adversary will not undertake the action. Geers further describes Schelling's three requirements of any successful deterrence strategy – capability, communication, and credibility – and applies them to denial and punishment strategies.[6] Capability is the actor's ability to prevent or punish an adversary; communication is accurately conveying that capability to the adversary; and credibility is whether the adversary believes the threat.[7]

Martin Libicki described the aims and methods of deterrence and discussed their application to the cyber domain in his RAND study, *Cyberdeterrence and Cyberwar*. He claims "the aim of deterrence is to create disincentives for starting or carrying out further hostile action. The target threatens to punish bad behavior but implicitly promises to withhold punishment if there are no bad acts or at least none that meet some threshold."[8] According to Libicki, effective

[3] Carl von Clausewitz, *On War,* Michael Howard and Peter Paret, eds. and trans. (Princeton, NJ: Princeton University Press, 1976).

[4] Sun-Tzu, *The Art of Warfare*, Roger Ames, trans. (New York: Ballantine Books, 1993).

[5] Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

[6] Kenneth Geers, "The Challenge of Cyber Attack Deterrence," *Computer Law & Security Review,* 26 no. 3 (2010), 298.

[7] Schelling.

[8] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Project Air Force, 2009), 28.

punishment is a key part of an effective deterrence strategy.

James Lewis further expanded on the requirements of deterrence strategy, noting "the concept of deterrence rests on a series of assumptions about how potential opponents recognize, interpret and react to threats of retaliation. The fundamental assumption is that a correct interpretation by opponents will lead them to reject certain courses of action as too risky or too expensive."[9]

For state actors these assumptions typically hold true. If it is assumed that a state is a rational actor, then for a deterrence strategy where one state communicates its capability to deny or punish an adversary in a credible manner, the adversary state will respond and bargain (so long as the threat is clearly communicated and credible). While this assumption holds true for state actors, it is difficult to apply to sub-state and non-state actors, as such actors typically focus on cyber crime and cyber terrorism, not state-versus-state cyber warfare. Therefore, the aim of this paper is to analyze the practicality of cyber deterrence on a state level. The paper will make no attempt to apply cyber deterrence to sub-state and non-state actors.

United States Air Force Major General Susan Helms, in her review of a large-scale deterrence exercise conducted by the Air Force, summarized some of the underlying problems with deterrence in any domain. She stated that deterrence must be planned and conducted before any hostilities occur or appear imminent, and that, "an effective deterrence strategy is not one that is defined by actions within one domain, or one area of responsibility, or one nation."[10] She also reinforced Geers and Lewis's assertions that deterrence "must not be invisible"[11] or that it must be communicated to the adversary that is being deterred.[12] General Helms also commented on the need for deterrence strategists to understand the adversary's perspective and that effective deterrence strategies are continually evolving.

> To be effective at the strategic level, deterrence must be viewed through the lens of how your adversary views the geopolitical world. Deterrence is not static; effective deterrence strategies will morph under conditions of crisis, and the level of uncertainty about your adversary's decision process must be actively tracked and accounted for, or else you risk serious miscalculation and unexpected deterrence failure.[13]

Only by incorporating these elements can an effective deterrence strategy be formulated and successfully implemented in any domain.

Nuclear Deterrence

Although there are fundamental differences between nuclear, cyber, and other forms of deterrence, it is important to understand the context and application of nuclear deterrence in order to apply it to other domains. Nuclear deterrence represents the most widely researched and arguably the most successful implementation of deterrence theory in history and therefore demands careful analysis before attempting to establish a new deterrence strategy in cyberspace. Mike McConnell, the former director of the National Security Agency (NSA) and Director of National Intelligence (DNI) in a 2010 *Washington Post* article summarized some of the key elements of Cold War deterrence and attempted to relate

[9] James A. Lewis, *Cross-Domain Deterrence and Credible Threats* (Washington, DC: Center for Strategic and International Studies, 2010), 1.

[10] Susan J. Helms, "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain," *High Frontier: The Journal for Space and Cyberspace Professionals* 7, no. 1 (November 2010), http://www.afspc.af.mil/shared/media/document/AFD-101116-028.pdf (accessed January 25, 2012), 12-13.

[11] General Helms's claim holds true for most historical examples but fails to explain Israel's nuclear weapons program and uncommunicated deterrence strategy. The Israeli program may provide a useful case study for future applications of cyber deterrence, where states are unable to communicate a credible threat without compromising their capability.

[12] Ibid., 13.

[13] Ibid.

them to cyber warfare. "During the Cold War, deterrence was based on a few key elements: attribution (understanding who attacked us), location (knowing where a strike came from), response (being able to respond, even if attacked first) and transparency (the enemy's knowledge of our capability and intent to counter with massive force)."[14] These same elements summarize the main requirements and weaknesses with cyber deterrence. Attribution and location are essential to any deterrence strategy, as are response capability, and transparency, but each of these elements present unique problems when applied to the cyber domain.

While there are many similarities between nuclear deterrence and cyber deterrence, there are several important differences that present unique challenges in the cyber domain. First, nuclear deterrence during the Cold War was not as simple as many outside observers believe in today's post-Cold War world. There was a fierce debate between academia and policy makers, particularly during the 1950s and 1960s, about how to best implement a nuclear strategy. These discussions went through several evolutions of counter force versus counter value doctrine and eventually led to an American policy of assured destruction, which served as the basis for the theory of Mutually Assured Destruction.[15]

Second, nuclear deterrence typically relies on the use of nuclear weapons to deter another state from using nuclear weapons.[16] While such a strategy was unpleasant and difficult to contemplate, it did not require an escalation in conflict. Once nuclear war began, it would theoretically be easier for a decision maker to respond in kind with nuclear retaliation. This assumption may not hold true in cyberspace. In order for states to retaliate against a cyber-aggressor they may need to resort to conventional attacks in order to maintain proportionality and limit the attacks' effect, or if the initial aggressing state has little cyber infrastructure to hold at risk.

As the Department of Defense concluded in a working study on the 'Essential Elements of a Deterrence Strategy for Cyberspace,' "the best response to an attack through cyberspace in many cases will not involve a reciprocal attack back through cyberspace."[17] This assumption makes it difficult to apply conventional understanding of nuclear deterrence to cyberspace because it is hard to predict how decision makers will actually behave in critical moments of cyber warfare.

The third critical difference between nuclear deterrence and cyber deterrence is reflected in the fact that while nuclear deterrence strategy eventually led to the adoption of nuclear arms control measures and limitation treaties, it is unlikely that a similar international agreement on cyber disarmament will be reached. Nuclear deterrence only holds because most current nuclear powers declare their nuclear weapons capabilities and are assumed to behave rationally. Furthermore, the United States and Russia have signed several treaties limiting the development and deployment of nuclear weapons in order to maintain peace and stability in the hope of avoiding war. These treaties form the basis for various confidence building measures between states that help limit the likelihood of miscommunication and inadvertent escalations.

This problem led the Department of Defense to conclude that cyber attacks are "an unrealistic candidate for traditional arms control" because "it is difficult to prove or disprove that an adversary has a cyber-attack capability, making any sort of 'cyber disarmament' intrinsically unverifiable."[18]

Finally, cyber weapons are based on dual-use technology. While there are some technological similarities between nuclear weapons programs and peaceful civilian nuclear programs, there are also clear distinctions between the two that are easily discernable to weapons inspectors and other

[14] Mike McConnell, "To Win the Cyber-War, Look to the Cold War," *The Washington Post*, February 28, 2010.

[15] Lawrence Freedman, *The Evolution of Nuclear Strategy*, Third Edition (New York: Palgrave Macmillan, 2003).

[16] Helms, 13.

[17] Department of Defense, "Essential Elements for a Deterrence Strategy for Cyberspace," 3.

[18] Ibid., 8.

experts. Furthermore, there are a limited number of states that possess the resources necessary to independently develop nuclear weapons, and the countries that have these resources would be unable to quickly convert civilian programs into weapons programs without attracting international attention. Even the most advanced non-nuclear states would require months (if not years) to successfully convert from one program to the other, therefore making it much easier for current nuclear powers to monitor the limited number of nuclear-capable states and then react if such a conversion were to be initiated.

These issues lead to the conclusion that the attempt to draw extensive similarities between nuclear and cyber deterrence is not a reliable or correct approach to implementing a successful cyber deterrence strategy. It may be necessary to apply lessons learned from other types of weapons to questions concerning cyber deterrence and cyber weapons in order to gain a more complete understanding of the potential approaches and challenges of implementing a cyber-deterrence strategy.

APPLYING DETERRENCE THEORY TO THE CYBER DOMAIN

Although most academic research on deterrence deals with nuclear deterrence, there is a growing field of research on the practicality of applying nuclear deterrence strategy to the cyber domain. These writings present conflicting views on the practicality of the synergy between the two modes of war fighting but both share common background. General Helms stated that one of the most important conclusions drawn from a set of deterrence exercises conducted at Schriever Air Force Base was that "some lessons about deterrence from the Cold War era do not necessarily translate to the space and cyber realm."[19] Even if Cold War lessons of deterrence do not directly apply in the cyber domain they provide a useful framework for reference in addressing the problem of cyber deterrence and attempting to establish a functioning cyber deterrence strategy.

One of the key issues with cyber deterrence is establishing what types of threats should be deterred and how to deter them. The simplest division of cyber threats places them into three categories: nation-state threats, terrorist threats, and criminal threats. Terrorist and criminal cyber threats, while dangerous and costly, do not pose as serious of a national security threat to the United States as nation-state threats, and existing counter terrorism and law enforcement mechanisms are more appropriate to face the threat than the Department of Defense. Furthermore, responsibility for dealing with terrorist and criminal cyber threats has been primarily delegated to the Department of Homeland Security and the Department of Justice rather than the Department of Defense. As such, the Department of Defense and United States Cyber Command's (USCYBERCOM) focus centers around threats posed by nation-states. Therefore, the primary focus of a cyber-deterrence strategy is the Department of Defense's efforts to deter nation-state threats in cyberspace.

As nation-state threats are the focus of deterrence strategy, they need to be analyzed in more detail. State-based threats can be further divided into cyber espionage and cyber attacks. Cyber espionage threats are primarily focused on collecting information through cyberspace while cyber attacks are designed to damage information and systems and potentially cause physical harm.[20] In theory, cyber espionage threats should be handled similarly to traditional espionage threats through robust defensive and counter intelligence programs. Despite the theoretical virtues of such a division it is difficult to implement in practice due to the difficulty in distinguishing between cyber espionage and attack threats. Oftentimes, the capability for

[19] Helms, 12.

[20] Although there have not been many examples of cyber attacks causing physical harm to date, many influential policy makers, most notably Richard Clarke in his book, *Cyber War: The Next Threat to National Security and What to Do About It*, continue to project the potential for cyber engagements escalating to cause physical damage. Thomas Rid disagrees with Richard Clarke's assessment and claims "Don't fear the digital bogeyman. Virtual conflict is still more hype than reality." Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, March 1, 2012.

implementing a cyber attack is the same as for a cyber-espionage threat, and the only difference is the intent of the actor. Furthermore, there is the potential that a cyber-espionage threat could be misinterpreted as preparation for a cyber attack and could elicit a military response.

In order to apply Cold War lessons about deterrence to the cyber realm, there are several steps that the United States must take. Former NSA Director and Director of National Intelligence Mike McConnell argues that in order for cyber deterrence to work, America must express its intent to use deterrence, it must translate intent into capabilities, and the ability to "signal" an opponent about potentially risky behavior must be developed.[21] Although McConnell argues that the technology exists, there are many potential challenges with cyber deterrence that must be addressed to make it a viable defensive strategy.

Prevention or Retaliation

The two main schools of thought on how to use deterrence in any domain advocate retaliation (punishment) or prevention (denial). Former Deputy Defense Secretary William Lynn said that, "we cannot rely on the threat of retaliation alone to deter attacks; deterrence must be based on denying the benefits of the attack." [22] Kenneth Geers applied this to cyberspace by stating "this means improving defenses, so that launching an effective attack becomes more difficult and expensive, and improving resiliency, so that effects of an attack can be mitigated."[23]

Although Secretary Lynn advocated the use of denial in deterring cyber-attacks, most scholars agree that prevention is not sufficient in the cyber domain and that a more aggressive retaliation approach to cyber deterrence must be pursued. Geers argues:

> Denial is unlikely due to the ease with which cyber attack technology can be acquired, the immaturity of inter-national legal frameworks, the absence of an inspection regime, and the perception that cyber attacks are not dangerous enough to merit deterrence in the first place. Punishment is the only real option, but this deterrence strategy lacks credibility due to the daunting challenges of cyber attack attribution and asymmetry.[24]

Defense in cyberspace is further complicated by the decentralized nature of the Internet and the vast amount of data transmitted. According to a 2011 Cisco report, in 2010 there were 1.84 devices connected to the web per person in the world, and by 2020 Cisco predicts that number will reach 6.58 devices per person.[25] Cisco also estimates that by 2015 just less than one zettabyte of data will be transmitted annually over networks.[26]

The mass connectivity of devices, the large amount of data transmitted on a daily basis, and the decentralized nature of packet-based communication systems make it nearly impossible to implement a defensive strategy that is one hundred percent effective, and the cost of securing network systems to prevent all attacks would be unstainable. However, the difficulty of implementing a defensive or denial strategy for cyber deterrence does not mean that states should ignore defense.

Defense can be useful in limiting cyber terrorism and cyber crime but is not likely to prevent a well-funded nation-state or state-sponsored actors from compromising digital systems. States should continue to invest in cyber security and defensive systems but must recognize that, barring a

[21] McConnell.

[22] Geers, 6.

[23] Ibid.

[24] Ibid., 10.

[25] David Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group, 2011, 3.

[26] Arik Hesseldahl, "Cisco: The Internet Is, Like, Really Big, and Getting Bigger," All Things D, June 1, 2011. (This is approximately the amount of data that would fill 250 billion DVDs. (Cisco, "Visual Networking Index IP Traffic Chart"))

significant technological breakthrough, well-funded nation-state actors will be able to penetrate secure information systems, necessitating a punishment response.

Although the United States and many other nations have the capabilities to punish potential cyber aggressors, there are several other challenges to pursuing this type of strategy. Geers goes on to state:

> The trouble with a punishment strategy, however, is that governments are always reluctant to authorize the use of military force (for good reason). Deterrence by punishment is a simple strategy but one that demands a high burden of proof: a serious crime must have been committed, and the culprit positively identified. The challenge of cyber attack attribution, described above, means that decision-makers will likely not have enough information on an adversary's cyber capabilities, intentions, and operations to respond in a timely fashion.[27]

Furthermore, "Deterrence by punishment is a strategy of last resort."[28] States are typically reluctant to use any kind of military force unless there is a clear cause to do so. In addition, deterrence by punishment in the cyber domain faces the problem of identifying the attacker. Without the capability to attribute an attack, deterrence by punishment strategy becomes ineffective.

A punishment strategy is also difficult to implement based on political and moral concerns. Without clear attribution of an attacker, punishment could be perceived as an overreaction or could be misdirected at an innocent third party. The consideration of the use of non-cyber forces to respond to a cyber attack would further compound these concerns. The United States will require a high burden of proof before responding to a cyber attack with conventional force, and decision makers will struggle with the question of using conventional force to respond to a cyber attack. These questions could limit the credibility of a punishment strategy that is one of the essential elements of implementing any successful deterrence strategy.

Attribution

Michele Markoff, a senior policy adviser in the State Department's Office of the Coordinator for Cyber Issues, succinctly summarized the importance of attribution in deterrence strategy when she said, "classic deterrence policy fails in the absence of attribution." She went on to state, "attribution, the ability to determine who is attacking you, is difficult but not impossible in cyberspace."[29]

Although the Department of Defense is working to improve its ability to attribute attacks, its attribution system is still not perfect and the Defense Department is assuming that following a large scale attack it will be forced to operate in a degraded environment, which will further hinder its ability to properly attribute attacks.[30]

Cyber attribution is also hindered by attribution challenges that are unique to the cyber domain. While it is easy to identify a conventional or nuclear attacker, identifying a cyber attacker is much more difficult. James Lewis stated that, "since we know the identity of an attacker in perhaps only a third of cyber incidents, and since a skilled attacker will disguise their identity to appear as someone else, the United States could easily attack the wrong target."[31] These uncertainties make it difficult to make a credible threat necessary for deterrence outside of conventional or nuclear conflict.[32]

General Helms summarized these problems.

---

[27] Geers, 9.

[28] Ibid., 6.

[29] William Jackson, "Cyberspace: A Battlefield Where the Old Rules Don't Apply," *Government Computer News*, 1.

[30] Ibid.

[31] Lewis, 1.

[32] Ibid.

> We are all aware of the challenges of attribution, and yet the measure of your deterrence campaign's success or failure depends on it. Without confidence of attribution, how do you credibly assure an adversary in a pre-crisis environment that you intend to respond? How do you mitigate the risk of a third party exploiting the ambiguity to create or escalate the crisis? How can you assess the success of meeting your deterrence objectives and adjust your adversary-focused campaign accordingly, if you are not confident about attribution?[33]

The questions General Helms posed accurately reflect the main problems with cyber deterrence and provide an excellent roadmap for what the United States needs to do to implement a successful deterrence strategy.

It may be possible that a cyber attack will be accompanied by kinetic action or other events in the international system that will help with attribution of a cyber attack.[34] For instance the 2007 cyber attacks on Estonia coincided with a diplomatic dispute between Russia and Estonia, suggesting that the attacks originated in Russia, although it remains difficult to determine if the attacks were state-sponsored or perpetrated by groups sympathetic to Russia that were not sponsored by the Russia government. A similar situation occurred in 2008 during the Russia-Georgia War. During this conflict the attacks on Georgia's internet infrastructure were most likely coordinated by Russia's Foreign Military Intelligence agency (GRU) and Federal Security Service (FSB), but the evidence is still not concrete and may not have been definitive enough to justify a counterattack on Russian targets were it not for the kinetic actions taken by Russia against Georgia.[35]

Overreliance on external events could also provide its own set of difficulties as other actors could seek to exploit a difficult international situation or further confuse the situation by launching additional attacks.[36] Third party actors could exploit a tense international situation through cyber attacks or conduct attacks that, as a result of false attribution, could escalate the conflict.

Some of these dilemmas could be mitigated through robust intelligence collection efforts. If the United States is unable to attribute an attack through cyber forensics, it may be able to attribute the attack through intelligence sources. It is important to bear in mind, though, that reliance on such systems would require real-time coordination between the intelligence community and military authorities, which is not always seamless.

The current construct and close relationship between USCYBERCOM and NSA likely makes such coordination practical but may become more difficult as NSA comes under increased scrutiny following recent leaks and when USCYBERCOM and NSA become more independent from each other in the near future. The commander of USCYBERCOM and the Director of NSA most likely will become separate positions following General Keith Alexander's retirement in the Spring of 2014.[37]

Capability, Communication, and Credibility of Cyber Deterrence

The final difficulty with cyber deterrence is the question of rationality and proportionality of response. James Lewis argues that in order for the United States to make a credible threat of retaliation, it needs to expand its options into

[33] Helms,14.

[34] Department of Defense, "Essential Elements for a Deterrence Strategy for Cyberspace," 8.

[35] John Leyden, "Russian Spy Agencies Linked to Georgian Cyber-Attacks: Follow the Bear Prints," *The Register*, March 23, 2009.

[36] Department of Defense, "Essential Elements for a Deterrence Strategy for Cyberspace," 8.

[37] Despite predictions of the split of NSA and USCYBERCOM, the commander has remained duel-hatted under Admiral Michael Rogers.

some other domain, but he also recognizes that such a response will escalate the conflict and present a new set of problems.[38] Matthew Crosston agrees that cyber-attacks can be easily viewed as an act of war and that attribution is essential because cyber-attacks can quickly lead to physical consequences.[39] A January 2013 report conducted by the Defense Science Board for the Department of Defense entitled "Resilient Military Systems and the Advance Cyber Threat" recognizes the potential for the escalation of cyber engagement in the future and recommends that the Department of Defense develop the capability to retaliate against a cyber attack with all elements of national power, suggesting that the United States needs to prepare to escalate a conflict beyond the cyber domain in order to maintain credible deterrence in cyberspace.[40]

The most conventional logic is to respond to a cyber attack with a cyber counterattack of some kind. Assuming the attribution problems are overcome, a state can counterattack in cyberspace similarly to how it would counterattack in any other domain. The difficulty with a cyber counterattack arises with Schelling's three requirements of a successful deterrence strategy: capability to retaliate, communication of intent to retaliate, and the credibility of the threat.[41] Each of these elements presents a unique challenge in cyberspace, and they are not mutually exclusive.

The first retaliation difficulty in launching a cyber counterattack is maintaining the capability to respond. Cyber attacks are possible based on weaknesses in the system being attacked that allow the attacker to penetrate it. The vulnerabilities to exploit are continuously changing as states patch security flaws and improve their defensive capability. Therefore, in order to maintain the ability to launch a cyber counterattack, the United States must continually search for weaknesses and develop exploits it can use against potential aggressors.

It may also be difficult to respond to a cyber attack if the attacker is not as reliant on cyber technology as the Untied States. A state's cyber vulnerability increases as the country becomes more reliant on information technology systems. If a state is not reliant on information technology, it may not be as vulnerable to a cyber counterattack as the United States is to a first-strike attack. These problems could be compounded following a cyber attack, which could limit the ability of the United States to respond to a cyber first strike. To overcome this difficulty, the United States must develop reliable second-strike cyber capabilities that will function following a catastrophic cyber first strike.

These three difficulties lead to the conclusion that the United States may need to respond to a cyber attack with a counterattack using other instruments of national power. A cyber attack may warrant a response with the conventional means of military power. Although there is some agreement that a kinetic retaliation to a cyber attack can be warranted, there are still concerns about the justness of such an action and the potential for quickly elevating the severity of the conflict. James Lewis claimed:

> Cyberspace poses a particular challenge for deterrence. State actors are engaged in harmful acts in cyberspace against the United States. However, military force is of limited utility in responding to or deterring actual cyber threats. A U.S. military response to espionage or crime would be a strange departure from international norms regarding the use of force. A retaliatory cyber attack (where the intention is to damage or to destroy, rather than exploit) or retaliation using a

---

[38] Lewis, 3.

[39] Matthew D. Crosston, "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly* 5, no. 1 (Spring 2010): 106, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf (accessed February 7, 2012).

[40] Department of Defense: Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, DC, January 2013.

[41] Schelling.

> kinetic weapon for a cyber attack against countries that have not used force against us or against individuals with criminal rather than political aims, could easily be interpreted as an aggressive and unwarranted act by the international community. The result is to cast doubt on the credibility of a retaliatory threat, weakening any deterrent effect.[42]

By this logic, regardless of justness of a retaliatory strike, the perception that the United States would not escalate a cyber-conflict into a kinetic fight limits the credibility of such a threat. Geers goes so far as to argue that a kinetic retaliatory attack may be more proportional than a cyber attack:

> One important decision facing decision-makers in the aftermath of a cyber attack would be whether to retaliate in kind or to employ more conventional weapons. It may seem logical to keep the conflict within cyberspace, but a cyber-only response does not guarantee proportionality, and a cyber counterattack may lack the required precision.[43]

Nevertheless, this assertion fails to address the political willingness of the United States to escalate the conflict and assumes that other states would believe America's threats.

Martin Libicki describes the escalation of conflict and defines what he refers to as the level of belligerence in conflict from least to most belligerent with respect to the use of diplomatic and economic force, cyber force, physical force, and nuclear force.[44] The United States and other nations are typically reluctant to elevate the level of belligerence from that of an attack suffered. This reflects the lack of credibility that the United States has when threatening to use nuclear weapons. Although most states believe that the United States will respond to a nuclear attack with nuclear action, they do not expect that the United States will respond to a conventional attack with nuclear weapons except for in certain limited circumstances. This is one of the important distinctions between cyber and nuclear deterrence. While a threat of nuclear retaliation for a nuclear attack is credible, the threat of nuclear retaliation for a kinetic attack or of kinetic retaliation for a cyber-attack may not be. In order for cross-domain deterrence to be used effectively, this view of American proportionality must be overcome.[45]

The second difficulty of implementing a cyber deterrence strategy is the ability to credibly communicate the threat of retaliation. Geers claims that in order for a denial or punishment deterrence strategy to work in cyberspace, it needs to be clearly communicated to the potential aggressors.[46] The difficulty with communication of a cyber retaliatory strategy is that clear communication of the capability to retaliate can compromise the exploit potentially used to retaliate. Therefore, communication of capability to respond to an attack can compromise the capability to respond.

Developing a strong cyber counterattack force and demonstrating its ability to respond in several engagements, thereby clearly communicating to other potential aggressors that the state has the ability to respond to cyber threats without compromising specifics on how the state intends to respond, could overcome this problem. This difficulty can also be overcome by communicating the intention to respond to cyber attacks with conventional forces, which are easier to identify and more difficult to defend against specific threats.

---

[42] Lewis, 1.
[43] Geers, 7.
[44] Libicki, 24.
[45] Crosston, 113.
[46] Geers, 298.

CONCLUSION

Cyber deterrence presents unique challenges and questions for traditional Cold War deterrence models. These issues require careful consideration by policy makers and strategists, as well as increased investment in cyber capabilities in order to respond to a variety of cyber threats. Cyber deterrence, like nuclear deterrence, requires multiple responses and actions depending on the situation and how the United States plans to respond. The best option is for the United States to develop multiple capabilities, cyber and non-cyber, in order to maintain its ability to respond regardless of the threat it faces. This approach is similar to Herman Kahn's concept of escalation dominance in nuclear war, which he defined as

> [The] capacity, other things being equal, to enable the side possessing it to enjoy marked advantages in a given region of the escalation ladder…It depends on the net effect of the competing capabilities on the rung being occupied, the estimate by each side of what would happen if the confrontation moves to these other rungs, and the means each side has to shift the confrontation to other rungs.[47]

The United States needs to develop and maintain the capability to be dominant at all levels of conflict escalation in order to deter potential aggressors. The United States currently possesses these capabilities at higher levels of conflict escalation but needs to develop and maintain its dominance in cyber warfare as well.

The United States has already invested significant resources into offensive and defensive cyber capabilities, and while the exact nature of these forces is not public knowledge, it is generally assumed that the United States maintains robust cyber forces that are as capable if not more capable than any other force in the world. This investment could explain why large-scale cyberwar, although predicted by pundits for several years, has yet to materialize. The United States may already be perceived to possess strong enough cyber and conventional forces to maintain escalation dominance, which deters potential aggressors in cyberspace. If this is the case, the United States needs to continue to invest in these capabilities in order to maintain escalation dominance and prevent other states from developing asymmetric advantages that could be used against the United States.

These assumptions are all based on attempts to apply nuclear deterrence theory to cyberspace, which although feasible in theory may differ in practice. A more applicable similarity may be the relationship between chemical or biological weapons programs and cyber weapons. All three are dual-use technologies that are simple to develop from civilian technology, easy to conceal, and can be adapted to a diverse set of targets. The Department of Defense also suggests there are similar difficulties in use between biological and cyber warfare: both "have the potential challenge of gaining access to specific targets, yet both can be applied indiscriminately across a wide range of targets. Similarities between biological warfare and cyber attack also can include uncertainty about attack attribution, uncertain effectiveness, the persistence of damaging results, and unintended consequences."[48] These similarities present a new framework for potential analysis of cyber deterrence and may lead to different conclusions.

Overall, cyber deterrence presents many unique challenges, but applying traditional deterrence concepts to cyberspace can help to overcome the difficulties in implementing a successful deterrence strategy. The most difficult questions and debates do not center on the practicality of cyber deterrence but on the assertion that the threat of cyberwar may be overblown and that deterrence may not be necessary in cyberspace.

If cyberwar proves to be less likely than anticipated, the United States may need to increase its investment in lower-level cyber crime and cyber espionage threats and decrease its

[47] Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965), 290.

[48] Department of Defense, "Essential Elements for a Deterrence Strategy for Cyberspace," 9.

emphasis on cyberwar. If this is the case, traditional modes of warfighting will prove more significant than cyber concepts. If cyberwar, however, proves to be the way of the future, cyber deterrence will prove indispensable in order to "subdue the enemy without fighting."[49]

[49] Sun-Tzu.

Terror on High: Deterring ASAT

Stephen Shea, Mathew Johnson, and Alfredo Zurita

Layered deterrence and carrot-and-stick diplomacy are the main ingredients for deterring ASAT.

As technology becomes even more pervasive in daily life, valuable and relatively vulnerable space assets will inspire greater desire to attack U.S. power through space.[1] As a result, Anti-Satellite (ASAT) deterrence, a fledgling area of study, will need to be developed and addressed in detail. The proceeding essay will attempt to answer the following questions. What motivates space attacks? How will the enemy try to attack our space assets? What can be done to deter future ASAT attacks?

REASONS TO ATTACK SPACE ASSETS

Despite the precedent of peace in space, there is still the worry that these assets will be attacked. These fears are justified for several key reasons, including the limited orbital slots available for satellites and common designs among adversaries to blind the United States, challenge American hegemony in space, and fashion an asymmetric response to U.S. military actions. While no nation has of yet struck another nation's space assets, the capability to do so has been repeatedly demonstrated.

As the need for global telecommunications continues to rise, the space available in Geosynchronous Orbit (GEO) becomes smaller and more valuable. As of February 2014, there were 391 satellites active in GEO.[2] The current issue with this orbital region is that, while the satellites are not in significant danger of hitting each other, there is a required level of separation between assets to ensure there is no interference or overlap in telemetric frequency. Mission and environmental requirements cause GEO satellite contracts to cost well into the billions of dollars; each of these represents a significant investment for corporations as well as the host nation. Moreover, countries near the same longitude will desire the same sliver of the GEO ring and will have to voice their arguments to the International Telecommunication Union (ITU).[3] Losing this competition over a scarce resource could lead to ASAT attacks from certain leaders. If done a certain way, ASAT could incapacitate valuable regions of GEO.[4]

Historically, one of the driving factors in the research of space technology is the military benefits. One of these benefits is the capability to observe an enemy nation without an air-breathing platform, that is, without the risk of a pilot's life or materiel. Knowledge of troop and equipment movements, for example, is invaluable during war; therefore, a nation has strong incentive to disable an enemy/rival nation's space capabilities through ASAT methods. The incentives only increase for utility satellites such as those of the Global Positioning System (GPS) that aid weapon targeting and ship movements.

---

[1] 2LT Stephen Shea is studying at the Air Force Institute of Technology (AFIT), Civilian Institute Program: Massachusetts Institute of Technology; 2LT Mathew Johnson is studying at the Air Force Institute of Technology (AFIT), Civilian Institute Program: Northeastern University; 2LT Alfredo Zurita is studying at the Air Force Institute of Technology (AFIT), ENY3 (Dept. of Aeronautics and Astronautics). All three are 2014 graduates of the U.S. Air Force Academy.

[2] Eric Johnston, List of Satellites in Geostationary Orbit, last modified February 21, 2014, http://www.satsig.net/sslist.htm, (accessed April 23, 2014).

[3] Graham Templeton, "What is Geostationary Orbit and Why is it so Important?" last modified December 14, 2013, http://www.geek.com/science/geek-answers-what-is-geostationary-orbit-and-why-is-it-so-important-1579225/, (accessed April 21, 2014).

[4] If satellites are destroyed in a manner that causes large amounts of debris, the debris would occupy valuable geostationary orbits.

With the U.S. having launched approximately 40% of the satellites currently active today, it holds the global lead for investment in space assets.[5] Some space experts and U.S. political advisers have reasoned for the U.S. domination of space. In short, they have argued to make space a U.S. controlled resource and to selectively choose who can and cannot gain access.[6] Such a statement is clearly unsettling to other national space agencies. These agencies are already occupied with internal politics and funding. Having outer space policed would cause great distress and international strife. The level of discomfort could result in other nations pushing back against the hegemon of the space domain and attempting to destroy U.S. military or commercial assets. Indeed, if the U.S., or any other nation for that matter, were to decide it would be the arbiter of what is allowed in orbit, one of the first logical steps would be to clear any opposition assets from the newly claimed area.

An additional reason nations may attack space assets would be in retaliation for military actions. These actions may or may not have been space-related to begin with—they could involve 'cross-domain' coercion--but an aggrieved nation might see fit to retaliate against the attacker nation's space assets. These nations may resort to ASAT operations, at a minimum to blind partially the attacking nation and thus curb the effectiveness of the original attack. In any case, before long, both nations involved may be utilizing ASAT capabilities and, as such, they will be interested in counter-ASAT capabilities to protect what remains of their own resources.[7]

TYPES OF ASAT TECHNOLOGY

Before international actors can become a threat, they need more than just the desire to destroy U.S. space assets. They need the capability. However, this is easier than it appears, for there are a multitude of ASAT methods, which can be condensed into five types: signal/intelligence disruption, terrestrial attack, kinetic annihilation, rendezvous disabling, and electromagnetic pulse.

The most accessible type of ASAT capability is signal/intelligence disruption. The easiest method of countering space assets is jamming, for it can be done with simple equipment for a low cost. This is useful to disadvantaged actors but has much lesser effect than other types of attack. Another ASAT method of this category is using lasers to blind optical sensors, often used by non-space powers. The last method is 'spoofing', or sending false commands. What distinguishes spoofing from a cyber-attack is that sending false commands does not involve unauthorized network access or software code manipulation.[8]

All of these methods are typically temporary; outside the space-time window of effect, the satellite is at full functionality. They also are traceable, due in part to their lack of destructiveness, but direct retaliation is not an option. The international community does not consider military strikes in space to be a proportional response. Countries like Iran already take part in these ASAT methods without receiving U.S. retaliation, so there already are

[5] Union of Concerned Scientist, UCS Satellite Database, http://www.ucsusa.org/nuclear_weapons_and_global_security/solutions/space-weapons/ucs-satellite-database.html#.VP0Jg_nF9p8, (accessed March 8, 2015). Peter Apps, "Global spending on space falls, emerging states are spending more," http://in.reuters.com/article/2014/02/13/space-spending-idINDEEA1C0I120140213, (Accessed March 8, 2015).

[6] Michael Cooney, "US Lab Developing Technology for Space Traffic Control," last modified January 23, 2014, http://www.networkworld.com/community/blog/us-lab-developing-technology-space-traffic-control (accessed April 20, 2014). Dolman, Everett C., *Astropolitik: Classical Geopolitics in the Space Age* (London: Frank Cass, 2002).

[7] Today, it is hard to imagine a splendid first strike that would incapacitate all or most satellites of a space power. Unlike the case of declining numbers of nuclear weapons, a nation's growing numbers of satellites are always widely dispersed and never 'in port'. After a strategic first strike—a space Pearl Harbor—there are likely to be many surviving satellites for the United States to defend.

[8] Micah Zenko, "Dangerous Space Incidents," http://www.cfr.org/space/dangerous-space-incidents/p32790 (Accessed 19 April 2014).

precedents for inaction.[9] For now, signal/intelligence disruption must be countered technologically, not kinetically or politically, through cross-domain deterrence.

Terrestrial methods for ASAT are those that attack the ground element of space operations, which includes ground infrastructure attacks and cyber-attacks. This type, while it does pose a significant threat, is covered under other realms of international law and requires different responses. Military strikes against ground stations count as attacks against sovereign soil of the targeted nation, which clearly justify military retaliation of the attacked country. Cyber-attacks involve a different operational domain than space and have different legal restrictions and military requirements than the space domain. Less formal differences between the domains include how easy it is for the aggressor to stay anonymous and who is capable of such an attack.

Multiple space powers have developed highly destructive ASAT weapons using kinetic annihilation, which include attack satellites and ground, aircraft, or ship–based antisatellite missiles. While the launch platforms of antisatellite missiles are quite different, the use and technology required are very similar. The missile is launched on a sub-orbital, intercept course and collides with a target satellite, completely destroying it. Both the United States and China have demonstrated this capability. The other developed system is an attack satellite, the Istrebitel Sputnikov. This Soviet satellite was designed to be rapidly launched from storage, approach a target satellite, and launch projectiles at the target satellites.[10] It is unclear whether Russia still holds this capacity. For both of these methods, a single collision is all that is necessary to completely destroy the target. Both of these methods cause the kinetic annihilation of the target.

The benefits of kinetic annihilation ASAT for the attacker include having the concept of operations well-grounded in a long tradition of military flight operations and, specifically, having possession, or full control and maintenance, of assets on the ground before an attack order is initiated. Most important of all, in contrast to signal disruption or terrestrial methods, if a kinetic attack succeeds as planned, the target is unrecoverable: the adversary's space platform will not be coming back online.

For some of the same reasons, this type of ASAT attack is the most critical to defend. China's 2007 ASAT demonstration created 2,300 traceable pieces of debris. This represents a significant percentage of the approximately 21,000 objects currently tracked.[11] In almost 60 years of space flight, approximately one out of nine tracked objects is debris from the Chinese ASAT event. While two U.S. ASAT tests created significantly less debris, it only takes one kinetic annihilation event like the Chinese demonstration to increase significantly the traceable debris in orbit. This does not account for all the smaller pieces of debris that can be just as damaging because all objects are traveling at incredible speeds.

While there have been few collisions in space, the odds jump with each ASAT kinetic annihilation event[12]. Without strong disincentives against this method, space will become increasingly dangerous. For both U.S. interests and the global good, ASAT demonstrations like the Chinese ASAT ought to be discouraged. Kinetic annihilation tests themselves must be deterred or at least performed in a way to keep orbital slots navigable.

These methods have a characteristic, which should make them easier to deter: they are practically impossible to hide. The United States and other nations have the ability to detect all space launches as part of their nuclear deterrence infrastructure. For this reason, outside of a hot war

[9] Micah Zenko, "Dangerous Space Incidents."
[10] Anatoly Zak, "The Hidden History of the Soviet Satellite-Killer." http://www.popularmechanics.com/technology/military/satellites/the-hidden-history-of-the-soviet-satellite-killer-16108970 (Accessed 18 April 2014).

[11] NASA.org, "Space Debris and Human Spacecraft," http://www.nasa.gov/mission_pages/station/news/orbital_debris.html#.U1KtevldWSo (Accessed on 19 Apr 2014).
[12] NASA.org, "Space Debris and Human Spacecraft."

between superpowers, this type of attack is unlikely at the moment, but still, we must be prepared for the rise of less stable actors who desire to test in prelude to more aggressive moves.

A future type of ASAT might be rendezvous disabling. Physically disabling a satellite might use any of the following methods, all of which require finely controlled rendezvous. This type requires the most complex satellites. The first method is physically damaging critical systems of a target satellite. It would be the most advantageous to use a small satellite, centimeters in length at most. This method could use a claw to snip off solar panels or antennas, which could either kill the electrical power system or mute the communication system. Even less invasive would be snipping the connecting wires of either of these systems. This method could also use a thruster to disable sensitive electronics. Thrusting on an optical sensor would at a minimum contaminate the lens, ruining the target's capabilities.

Another futuristic method would use directed electromagnetic strike, essentially using focused electromagnetic energy to short circuit an individual spacecraft. A laser could be used to damage electronics in the same way as the claw method, cutting off components or wiring. The aggressor satellite could puncture a target with two spikes and run large voltages between the spikes. A satellite could also attack a target by sending radiation or strong electromagnetic signals to disrupt and damage the target's inside wiring and systems. These abilities are likely to be development intensive compared to other methods. This would require a less precise rendezvous, but a much higher power demand, leading to a larger satellite.

The benefit of electromagnetic strike over kinetic annihilation is the target is disabled without creating a debris cloud. This lessens the international damage and thus the backlash of such an action. International actors that would use this method will likely try to evade detection, plausible with a tiny satellite or in the correct window of opportunity. They would hope to damage vital space assets free of accountability like actors do in the cyber realm.

For many systems, it may be impossible to damage wires without disconnecting the component, but if an actor is able to damage wiring or internal systems, an attack could be hidden as a spacecraft malfunction. Close inspection of satellites, which may be the only way in some cases to tell the difference between attack and malfunction, is expensive and difficult due to the nature of the space environment. Whether a component is damaged or cut off, it is most important to know rapidly two things: that an attack actually took place and the identity of the attacker.

The last and least likely type is an Electric Magnetic Pulse (EMP). The only known human cause of an EMP is nuclear weapons, discovered during high-altitude nuclear tests in the 1960's.[13] Even limited powers in the space and nuclear arenas like North Korea might be capable of an EMP, but limited nuclear materials also make a secondary target like space unlikely. Nuclear weapons would be much more devastating to ground targets. Also, nuclear detonations in space are now clearly forbidden by international law and would surely bring the wrath of most powers around the world, particularly space powers that would be damaged in the attack.[14] Space powers have even greater disincentive because they would be directly damaging themselves. If non-nuclear EMPs are possible, the best delivery would be similar to rendezvous attack, with a smaller area of effect due to power constraints and ability to focus against individual satellites.

Each of these ASAT methods holds a different challenge to deterrence. Signal/intelligence disruption will not be covered by most deterrence methods because of its low permanent impact to space assets. Terrestrial and EMP attacks spill over into other national security realms, so they will at least be partially included in standard

[13] "Nuclear Weapon EMP Effects," http://www.fas.org/nuke/intro/nuke/emp.htm (Accessed on 19 April 2014).
[14] UNODA, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, http://www.unoosa.org/pdf/publications/ST_SPACE_061Rev01E.pdf, (accessed March 9, 2015).

deterrence strategies. The ASAT types most critical to deter, today, are kinetic annihilation and rendezvous disabling. Building international consensus against kinetic annihilation will be easier than rendezvous disabling due to kinetic attacks' greater physical damage to the space environment. Yet, both are equally damaging to a peaceful and cooperative space environment.

DETERRENCE IN SPACE

Deterrence, in essence, is the act of preventing conflict escalation through intimidation, coercion, or fear of consequence. It is important to distinguish that deterrence involves avoiding attacks and should not be likened to diminishing an adversary's capabilities.[15] To establish the framework, there are three requirements for deterrence. First, the enemy must believe that their actions will be identifiable; otherwise, logic would preclude the absence of any negative consequence for the aggressor.[16] Next, the adversary must also be risk adverse. This is essentially synonymous with assuming rationality, a factor that is frequently mentioned and discussed in nuclear deterrence theory. It is impossible to deter an irrational actor who does not fear retaliation. Last and most difficult, the risk must outweigh the cost of aggression. The actor must believe that attacking will result in an adverse response with losses greater than the expected gain.

The space environment is unique and should be given distinct consideration in analysis. Space assets in low earth orbit (LEO) are moving at about 17,500 miles per hour and are subject to several extreme conditions. These conditions such as near vacuum pressures, free-fall, radiation, and extreme temperature vacillation make designing and placing assets in space exceedingly difficult. As discussed previously, the motivation for attacking space assets is there; the problem lies in preventing possible attacks. First, it is important to understand why conventional deterrence techniques might not work and what hindrances might be faced.

In addressing the first requirement of deterrence, the enemy must believe that the attack can be traced back to them. The space environment, while vast, is becoming more and more populated as technology along with the probability of accidents increase. Currently, there are over thirteen-thousand man-made objects larger than ten centimeters in diameter orbiting the Earth that are being tracked by the U.S. Space Surveillance System (SSS).[17] The SSS, in conjunction with systems at Cavalier Air Force Station and Eglin Air Force Base, provides a capability of space awareness that is both rare yet slightly limited—the systems are not infallible and have weaknesses.

One limitation of the systems in place that the enemy may try to utilize is the objects being tracked cannot be monitored for the entirety of their orbits. Instead, they are usually identified upon detection, and, using two sets of range and timing data, their orbital parameters are updated a few times per orbit. An ASAT attack could hide in the blind spots of space situational awareness. Without adequate surveillance, a sudden loss of satellite functionality or communication could be difficult to diagnose. For example, if rendezvous disabling at LEO can be conducted swiftly and during the anonymity time window, there is little to no deterrence available for the attack. The only possibility is to narrow down suspects to those who possess such a capability.

Assets in GEO are less numerous, but given an altitude of about 36,000 km, they are also harder to observe. With proliferation of advanced

---

[15] Karl Mueller, "The Absolute Weapon and the Ultimate High Ground: Why Nuclear Deterrence and Space Deterrence Are Strikingly Similar - Yet Profoundly Different," *Anti-satellite Weapons, Deterrence and Sino-American Space Relations* 1 (2013): 42; http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf (accessed April 26, 2014).

[16] James Lewis, "Reconsidering Deterrence for Space and Cyberspace," *Anti-satellite Weapons, Deterrence and Sino-American Space Relations* 1 (2013): 73; http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf (accessed April 26, 2014).

[17] "Orbital Objects, Satellites, Space Junk Information, Facts, News, Photos -- National Geographic," National Geographic, http://science.nationalgeographic.com/science/space/solar-system/orbital/ (accessed April 26, 2014).

technology, an attack in GEO could increase in likelihood with a larger window of attack, especially if the limits on GEO situational awareness endure. Also, assets in GEO tend to be more valuable due to the advantages of the orbit for communications and early warning. Anonymity is a complicating factor made larger by limited space situational awareness. There are possible windows of attack where the enemy can escape repercussions and ultimately deterrence.

The second requirement of deterrence, a rational actor, cannot be established through previous crisis behaviors; however, it may prove a surprisingly workable assumption. Stability in state actors' behavior patterns, defined by slow change, is a function of the difficulty inherent in acquiring significant space assets and technology. The likelihood of an undisciplined or reckless actor acquiring said technology is most present in stealing low-budget jammers and non-kinetic weaponry. However, with growing technology, more and more states are developing space capabilities.

In the case of North Korea, it already has a space program with a successful launch in 2012. Many believe its purpose is to develop ICBMs, but with additional testing and design, their program could be repurposed for ASAT.[18] Plus with North Korea's ties to Iran and other destabilizing actors, the spread of technology could eventually lead to space assets for kinetic attack falling into the hands of 'irrational actors' with little concern for customary constraints of the international system.

The final requirement, that the risk must be greater than what might be gained, is the most elusive. There are several unique features of the space environment that may make attacks more beneficial than was the case for nuclear deterrence on the ground. A fundamental difference between nuclear deterrence and space deterrence is the sheer destructive power of the assets involved. A nuclear attack risks both structural and more importantly human capital. It affects the adversary on numerous levels, psychologically, economically, and militarily.[19]

With a space attack, the immediate damage is narrower, to an expensive and valuable asset leading to a loss in capability such as GPS coverage or military surveillance. The gain from a strategic space strike for a technologically inferior foe may be extremely valuable in a military conflict. Due to the difference in consequences, however, the international reaction is likely to be limited in scale when compared to a nuclear attack, and, especially for a revisionist state, it is much easier to justify an attack without human casualties.

When considering a military response to attacks on a space asset, counterattack options are few. Scorn from the international community has not stopped North Korea from going nuclear, so it is unlikely to affect the spread of ASAT capability. Also, it would be hard to justify a disproportionate military attack on a space aggressor, to audiences abroad or at home, that would be severe enough to provide deterrence. With regard to proportional strikes, the attacker in a likely scenario might not possess significant space assets for the defender to retaliate against. Thus, with the increasing importance of our space assets, the gain for others in attacking them, especially without proper precautionary actions by the United States, can outweigh the cost.

Another deterring factor that exists in the nuclear realm is the so-called first-strike taboo. A possible reason why a nuclear attack has not occurred since 1945 is that no nation wants to carry the burden of first strike that could plausibly lead to a general nuclear exchange in which everyone lost.[20]

---

[18] Duyeon Kim, *North Korea's Successful Rocket Launch*, http://armscontrolcenter.org/issues/northkorea/articles/north_koreas_successful_rocket_launch/ (Accessed 27 April 2014).

[19] Karl Mueller, "The Absolute Weapon and the Ultimate High Ground: Why Nuclear Deterrence and Space Deterrence Are Strikingly Similar - Yet Profoundly Different," *Anti-satellite Weapons, Deterrence and Sino-American Space Relations* 1 (2013): 47; http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf (accessed April 26, 2014).

[20] Bruce MacDonald, "Deterrence and Crisis Stability in Space and Cyberspace," *Anti-satellite Weapons, Deterrence and Sino-American Space Relations* 1

Though this factor is probably small compared to likely nuclear retaliation, this first-strike aversion does not even exist in the space realm. The only casualty is a space asset unknown to the nation's people, and its loss may not readily affect them, depending on the satellite's purpose. While long-term effects of ASAT attacks are crippling to global infrastructure for communications and navigation due to increased debris and collisions, short-term effects do not provide significant adverse consequences. If ASAT capability exists and the need is present, neither fear of retaliation nor first-strike taboo are likely to be strong enough deterrents.

A PLAN FOR SPACE DETERRENCE

Given the uniqueness of the space domain and the hindrances to deterrence identified, actions that can be taken will require complex tradeoffs. The approach should be multifaceted, catering to powerful nations already in space and those with intentions of acquiring future space capabilities. To do this, our proposed plan incorporates a carrot-and-stick method to incentivize peaceful space operations as well as discourage ASAT attacks.

First step is we must minimize the gain inherent in any space attack. There are numerous actionable methods for the U.S. to protect itself. For example, in order to protect crucial space assets, while it will be more expensive, space platform architecture should be distributed. A valuable and strategic asset to the military is encrypted and secure communication. The capability should not rely on one robust and hardy satellite but should be conducted by a disbursed network. With added redundancy, it is more difficult for an adversary to eliminate a U.S. capability. Terrestrial assets could be distributed and buried, following NORAD, to further reduce an attacker's potential gain. These methods of distributed architecture minimize the reward of successful ASAT attacks.[21]

The hardiness of each satellite can also be increased. First of all, the U.S should continue to provide crucial assets with nuclear radiation resistance and long service lives. To combat ASAT methods, additional capabilities can be added. For example, with the expansion of microsatellites, they can eventually be made to orbit or perform proximity operations for a larger satellite. They can act as sensors and perform countermeasures to protect the larger platform. After a threat is detected, the micro-sat can be designed to respond using a variety of methods, including sacrificing itself or (someday) employing ionic fluid deflection.[22] Lastly, the micro-orbiter can be used for state-of-health monitoring and troubleshooting.

Other hardiness measures include cameras used for proximity visuals and threat detection, and mini-thrusters for additional agility. The agility is gained by having more robust onboard propulsion and control in order to navigate and avoid threats. This can be useful in protecting against some rendezvous disabling methods. Increased detection and movement could dissuade an aggressor by forcing him to meet high satellite control requirements.

Increased space situational awareness is also critical for strengthened deterrence. Upgrading U.S. space surveillance capabilities to close the holes in awareness at LEO and GEO would help hold aggressors accountable and allow for greater countermeasures. Research into this and other protective technologies should be bolstered to develop essential capabilities that increase deterrence.

Reducing the gains from attack is an ongoing effort as well as one that should be researched for

(2013): 84; http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf (accessed April 26, 2014).

[21] Bruce MacDonald, "Deterrence and Crisis Stability in Space and Cyberspace," *Anti-satellite Weapons, Deterrence and Sino-American Space Relations* 1 (2013): 91; http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf (accessed April 26, 2014).

[22] Thomas Joslyn, information received by author, Rocket Propulsion Class Lecture, USAFA, May 3, 2013. Ionic fluid deflection is an experimental concept that would use vector ionic liquids as a momentum transfer medium to perturb incoming objects away from the primary satellite.

more effective technologies. However, a smaller gain may not be a complete disincentive. Therefore, a retaliatory stick is necessary for the carrot-and-stick approach to work. Denial of access to the domain itself in response to successful or even attempted aggression might instill fear in would-be attackers.

The major space powers, the United States, Russia, and now China, have the technical wherewithal to execute kinetic ASAT exercises as a demonstration of power and of their willingness to deter space attacks by punishment. However, it has not been expressly stated how these ASAT capabilities will be utilized. If an agreement were made to use this capability for denying access to the space domain for any state or entity that acts aggressively, it might provide benefits that would have to be weighed against the costs and difficulties of maintaining agreement among enforcer powers as to who, in space, were the aggressors.

Everett Dolman points out in *Astropolitik* that an international space agency could be erected to oversee all actions and efforts conducted in the space domain.[23] This is politically unfeasible; even the United States would not allow others to search its satellites, but an international agency could serve to minimize excesses of unilateralism. This organization would determine when a country has crossed the line into 'aggression' and coordinate denial of space against the culprit. It would prevent the aggressor from gaining space technologies and from launching successfully, perhaps via the interception of its rockets.

Credible prosecution of this deterrence-by-punishment system would rely upon capabilities of countries like the United States, China, and Russia. The international organization could also oversee rehabilitation and eventual recertification of previous aggressors as well as probationary inspections of launches once the aggressor is permitted to reenter the space domain. Reinstatement would need to be a stringent and lengthy process to make deterrence work against ASAT.

To earn its keep, the anti-ASAT organization could also resolve space disputes and help regulate information and materials that could be used for ASAT capabilities. It should also set regulations for the disposal of satellites that are too dangerous to reenter the Earth's atmosphere on their own. The United States already set a precedent, albeit controversial, for this in 2008. Regulations would, as an alternative to far more cumbersome multilateral negotiations, outline what is considered dangerous and who is capable of properly disposing satellites while minimizing debris.

There is at least one major complication in punishment through space denial: Most countries will not stand for an attack against a manned launch, and the United States would not want to pull the trigger in this case either. There is still some benefit to preventing just unmanned launches. Manned launches cost more because of life support equipment and supplies, and most countries' space programs are not designed to function through purely manned launches. At a minimum, the aggressor country at least suffers additional economic cost for continuing a space program—even if manned launches are excluded from punishment.

Another objection to the "stick" of punishment by attacking unauthorized launches is that it is too risky for those that enforce denial of space access. Yet, as was the case for classical deterrence, harsh consequences are the only way to convey that the space domain is really protected and that assets should not be marginalized. One of the key principles of nuclear deterrence is still the risk of nation-ending destruction. While space does not have such an extreme without nuclear weapons in play, having a risk of escalation and punishment is needed to deter an aggressor in the first place. The aggressor must see the possibility of severe punishment as part of what makes the cost of ASAT too high to be worth the potential benefit.

For the carrot in this proposed plan, it is also important to incentivize peaceful space operations. There are many methods to approach this, some

[23] Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (London: Frank Cass, 2002).

already in place. First, international partnerships with not only nations maintaining large programs but those with smaller initiatives that might be pooled should be established or bolstered. The International Space Station is a prime example of the successes achievable through international efforts. The ISS acts as a stabilizing agent through the concept of self-defeat.[24] For example, if a country that participates on the ISS wanted to also conduct an ASAT attack on an asset in LEO, they might be dissuaded by the prospect of endangering their own assets whether human or technical. Also, such an attack would immediately jeopardize all programs conducted in the international effort due to repercussions that would follow.

Difficulties with "space aid" that may be anticipated include supplier restrictions on the distribution of proprietary information, as well as incompatible commercial or security interests among competing sovereigns, and endemic fiscal limitations. For this kinder, gentler approach to work with the United States as a spearhead, a reinvigorated interest at home in the space effort must be seen followed by an increased budget for space.

Another method of incentivizing budding space ventures as well as peaceful operations abroad could be offering other countries access to space assets in return for support in joint operations and work to improve their own space programs. Assets such as satellite communications, GPS, and satellite entertainment are very desirable to nations that do not currently possess said technology. This carrot has the potential to realize a global community committed to peaceful operations as well as effective, and profitable, space ventures through synergistic and cooperative efforts.

Ultimately, international commitment is critical to successful space deterrence. Deterring ASAT should not be a solely U.S. endeavor if its purpose is to sustain a peaceful environment for all nations. There is incentive for many nations to join a regime that includes both the carrot and the stick. Implementation of this plan requires an enormous international effort and will not be settled upon immediately.

At the same time, the harshness of the stick in this plan should not be alleviated in order to reach a watered-down, multilateral consensus. A true consequence needs to be established that will effectively deter ASAT attacks as the space domain becomes more and more accessible and the possibility of attack increases.
Also, peaceful access to the space domain should be promoted and proliferated. The proliferation of space assets can be stabilizing, a parallel to Waltz's concept of nuclear deterrence when every state accepts that something it values dearly is being held hostage, as collateral for good behavior.[25] Cooperative efforts, access to valuable space services, and induction into an elite group can be extremely exciting and motivating for a developing country.

Assuming success with an overwhelming majority involved in this international and eventually global space posture, the environment could be extremely intimidating, indeed forbidding, to a prospective aggressor. The hope is that in the long run, carrot-and-stick arrangements transition from a deterrence method to a governance system for establishing and maintaining stable and reliable access to space for the global community.

CONCLUSION

Space is, and will continue to be, a critical environment for both civilian and military operations. Due to its value to the United States and other nations, there are strong incentives for technologically inferior challengers to disrupt and destroy space assets. As more countries gain space capabilities, the environment will continue to become more crowded and more complex. It also has the potential to become more dangerous, for there are numerous ASAT methods that need to be deterred.

[24] Michael Krepon, "Space and Nuclear Deterrence," *Anti-satellite Weapons, Deterrence and Sino-American Space Relations* 1 (2013): 27; http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf (accessed April 26, 2014).

[25] Scott Sagan and Kenneth Waltz, *The Spread of Nuclear Weapons: A Debate* (New York: W.W. Norton, 1995).

An effective way forward consists of three parts: reducing the gain of ASAT; brandishing a stick for aggressors; and offering a carrot for peaceful sharing of the space environment. The most effective way to minimize the gain of ASAT attacks is distributing the space architecture. Using disbursed fleets of many satellites significantly lessens the impact of one ASAT attack. The stick punishing aggressors is subsequent denial of their using the space environment. Denial might be coordinated and executed by an internationally established space agency, which would take responsibility for shooting down aggressors' space launches, restricting technology from rogue actors in space, and sanctioning individuals involved in violating space law and regulations. Equally important is the carrot: building relationships between national space agencies and working on joint projects. Major projects like the International Space Station deepen ties between countries even when earthbound issues create tensions.

Deliberation and agreement among countries, particularly space powers, is vital to both the carrot and the stick of deterring ASAT attacks. The process should be led by the United States but will be useless without international buy-in. Compromise is necessary, but toothless agreements to attain a putative consensus will be ineffective. The world needs a peaceful and cooperative space environment, and the sooner an effective method of deterring ASAT is established, the closer we will be to a better future for both the United States and the whole of mankind.

Book Review
The Strategist: Brent Scowcroft and the Call of National Security by Bartholomew Sparrow (Public Affairs, 2015)

Schuyler Foerster

A popular new biography pays overdue tribute to a living legend.

Bartholomew Sparrow's rich and detailed biography of Brent Scowcroft—a still very active and now nonagenarian—has been on bookshelves since early this year.[1] Many, including those who have an intimate familiarity with some of the events and personalities in this book, have already offered thorough reviews of the work.[2]

The purpose of this review, therefore, will not be to shed new light on the biography but to focus on what this reviewer believes is the more enduring message of the narrative, and, indeed, the life of Brent Scowcroft.

Brent Scowcroft's life has been—and remains—one of commitment, hard work, and service to the nation above personality, political party, or personal preference. His legacy—as Sparrow details and with which others agree—is one of even-handedness and integrity. He has largely succeeded in managing the most difficult policy issues as well as some of the most difficult personalities in the policy world. Scowcroft is not, as Sparrow and other reviewers have noted, without error or misjudgment, but he nonetheless sets a standard for dedication to higher purposes, which Sparrow's biography celebrates.

Sparrow details Scowcroft's roots in a modest Mormon family, as well as Brent's own extraordinary work ethic as a young boy. His formative years were shaped by the run-up to World War II, and his instincts took him to West Point, from which he graduated in 1947. Too late to fight in World War II, he survived an almost fatal crash-landing in 1949 that ended his operational flying career and precluded a combat role for an individual ironically destined to play such an influential role in shaping national security policy.

---

[1] Dr. Schuyler Foerster is the Brent Scowcroft Professor of National Security Studies in the Eisenhower Center for Space and Defense Studies, Department of Political Science, U.S. Air Force Academy. The views expressed here are his own.

[2] As examples of some of the more substantive reviews of Sparrow's biography, see Hal Brands, "Bookshelf: Grand Strategy in the Real World," *The Wall Street Journal*, 23 January 2015, www.wsj.com/articles/book-review-the-strategist-by-bartholomew-sparrow-1422053450; Steve Donoghue, "Book Review: 'The Strategist,'" *Open Letters Monthly: An Arts and Literature Review*, www.openlettersmonthly.com/book-review-the-strategist/; Roger Harrison, "Book Review: 'The Strategist' by Bartholomew Sparrow," *Strategic Studies Quarterly*, www.au.af.mil/au/afri/review_full.asp?id=746; *Kirkus Reviews*, "The Strategist," www.kirkusreviews.com/book-reviews/bartholomew-sparrow/the-strategist-brent/; Daniel Kurtz-Phelan, "Sunday Book Review: 'The Strategist: Brent Scowcroft and the Call of National Security,'" *The New York Times*, 4 March 2015, www.nytimes.com/2015/03/08/books/review/the-strategist-brent-scowcroft-and-the-call-of-national-security.html; James Mann, "Book Review: 'The Strategist,' on Brent Scowcroft, by Bartholomew Sparrow," *The Washington Post*, 30 January 2015, www.washingtonpost.com/opinions/book-review-the-strategist-on-brent-scowcroft-by-bartholomew-sparrow/2015/01/28/36794714-9a83-11e4-a7ee-526210d665b4_story.html; *Publishers' Weekly*, "The Strategist," www.publishersweekly.com/978-1-58648-963-2.

The policy role that Scowcroft ended up playing began in academe under a formidable set of mentors—William T. R. Fox at Columbia and, in the famed "SOSH" (or "Social Sciences") Department at West Point, Col Herman Beukema and Col George "Abe" Lincoln. This was not the academe of theoretical debates, but of application of theory to a profession whose *raison d'être* was national security. The coin of the realm was "realism"—for Scowcroft, not realism devoid of moral content, but one that defines the boundaries in which moral purposes can be prudently pursued.

On the one hand, that instinct for realism produced a determination that the national security establishment be structured to identify complex relationships of power and the strengths and vulnerabilities not only of others but also of ourselves. Such a structure should not serve narrow individual, political, or bureaucratic purposes; rather, it should serve the President in the exercise of his constitutional responsibilities. Sparrow describes in immense detail Scowcroft's years of holding important staff jobs in the military, but which, for Scowcroft, was a world dominated by drudgery and bureaucracy.

In subsequent years—in restructuring the National Security Council (NSC) in the Ford Administration after Henry Kissinger left to be Secretary of State, and in rebuilding that structure as George H. W. Bush's National Security Advisor after the Iran-Contra debacle—one sees Scowcroft's concern for "process," not for its own sake but to ensure that the best analyses and competing recommendations find their way to the table, and are not shut out because of ego, stove-piped structures, or muzzled staffers. Issues need to be seen as they are, not as one wishes them to be; the best policies are often a mix of seemingly contradictory proposals (as in the Scowcroft Commission's delicate balancing of arms control and strategic force modernization to fit political realities of the early Reagan Administration). The policy apparatus—not just the 'guru' at the center—must be equipped to visualize both the realities and the opportunities.

That instinct for realism, of course, can also cloud one's vision. This reviewer recalls an interview on the *Today* show in spring 1989, when a major review of national security policy that Scowcroft had launched was coming to an end. When asked if the review was producing any new insights, Scowcroft replied, "We're not quite done, but it looks like the future will look a lot like the past, on a more or less straight line of projection." Sparrow highlights this period, and other reviewers note that Scowcroft's conservative instincts reinforced skepticism that Gorbachev was genuinely interested in effecting a major change in the U.S.-Soviet relationship. Then, when it became clear Gorbachev was so inclined, Scowcroft remained less enthusiastic about the opportunities and increasingly concerned about whether such changes could be managed.

Managing a "world transformed" (in the words of the memoir that Scowcroft co-authored with George H. W. Bush)—the end of the Cold War, the unification of Germany in NATO, and the demise of the Soviet Union—represented the consummate accomplishment of that Administration, one that subsequent generations can easily underestimate. The Bush national security team may not have envisioned the possibilities these changes might bring. Indeed, in later years, Scowcroft was openly skeptical about some of them, including the enlargement of NATO (a view he shared with George Kennan, who had been Ambassador to Yugoslavia when Scowcroft was Air Attaché). But that team was enormously effective in anticipating how these changes could be inherently destabilizing to the international order and in focusing on how to preserve as much stability as possible.

Scowcroft is the first to say that he is not a visionary. In 2011, at an Aspen Institute event in his honor, Scowcroft was asked about the secret of his success. Without hesitation, he replied, "I have always tried to surround myself with people smarter than I." If "smarter" means expertise, then Scowcroft did indeed focus on bringing people into his net—whether at the NSC or in his post-government consulting business—who were "smarter" than he. If "smarter" includes instincts about how ego and presumption can get in the way of a better outcome for a higher purpose, then there are few who are "smarter" than Brent Scowcroft.

Although Scowcroft's career quickly shifted from the military academic world of West Point and the Air Force Academy (where he served from 1962 to 1964, including as Acting Department Head in 1963-64) to the cauldron of policy making, a substantial part of his legacy will remain in the world of education. Sparrow details how Scowcroft's consulting business produced significant wealth, and Scowcroft has contributed substantially to a host of institutions, not all of which bear his name. At a dinner in his honor to inaugurate the Scowcroft Professorship in National Security Studies at the Air Force Academy, this reviewer asked him how he would charge the incumbent in that position. Without reservation, and in his typically understated way, he said, "Teach them *how* to think, not *what* to think." In Sparrow's biography, Scowcroft recalls a mentor many years prior who did just that for him. It is a value that transcends expertise and instills both perspective and an antenna for complexity.

Brent Scowcroft is a "heroic" figure in large part because he has endured and survived. On a personal level, Sparrow's biography tells the little-known story of how Brent provided home care for his wife, Jackie, during her 25-year long and burdensome illness, even while his time in government demanded all of his energy. No complaints; indeed, few even knew. Professionally, over the last half century, Scowcroft has worked with—and been buffeted by—some of the largest figures in national security policy. He has been at the center of countless key foreign policy decisions, for which he was the man in the background rather than the man out front. He challenged orthodoxy, but rarely people. He garnered respect from all sides of the aisle. He worked, it seems, harder and longer than anyone else. That reputation also enabled him to "speak truth to power," as when he warned publicly in August 2002 about the dangers of a precipitous invasion of Iraq—a position for which he was spurned by many but ultimately vindicated by history.

Sparrow quotes Scowcroft as saying there is "nothing better than to be working for something greater than you are." Many commentators have suggested that Scowcroft will not be remembered for the policies he shaped or the structures he reformed. In that respect, as one reviewer noted, he is a "transitional" figure. This reviewer suggests that this misses the broader point. We hope he will be remembered for the moral compass that underscored an unrelenting commitment to service, a determination to base policy on national interest grounded in the best analysis that can be brought to bear, and—most of all—an unwavering sense of his own humanity, and the modesty and compassion that comes with it. While we await Brent Scowcroft's own memoirs, we can thank Bartholomew Sparrow for introducing us to the man and reminding us of this all-too-rare legacy.

Publishers Corner
Manned Space Exploration: America's Folly

Roger G. Harrison

Advocates of manned space exploration have some explaining to do.

If we want to assess the benefits of human space exploration, particularly to Mars, who better to consult than the good folks at MIT, a place presumably bristling with engineering knowledge and human genius. Fortuitously enough, the "Space, Policy and Society Research Group" at MIT has produced a study on "The Future of Human Space Flight" for our edification and enjoyment. It is six years old at this writing, but the facts have not altered appreciably: the humans who would have to be transported to, sustained on, and returned from the red planet are the same frail and physically limited homo sapiens they have always been; they are still carbon-based life forms, and therefore dependent on oxygen and water; and they are still as certain to deteriorate and die after relatively short periods of exposure to gamma and other radiation at strengths present in space and (especially) on the surface of Mars.

What are the justifications for flinging such creatures into the vastness of space? The MIT report purports to provide some. Though the product of scientists, the study is not, in a strict sense, scientific. It is, rather, a piece of advocacy whose authors are intent on demonstrating that human space exploration is worth the admittedly high cost in lives and treasure. Still, there are obvious things that even these advocates feel constrained to accept. Hence their conclusion that, whatever the case for human space exploration might be, it does not include the advancement of scientific knowledge on the one hand, or the prospect of turning an honest dollar on the other.

This is the burden of the Study's identification of supposed "primary" and "secondary" objectives of human space travel. Interestingly, the authors identify as "secondary" all the possible tangible benefits, and as "primary" the intangible ones. By this reckoning, "science, economic development, new technologies and education" – in short, those things most widely touted as the "pay off" from vast investments necessary for human space travel – are "secondary" objectives, which the authors conclude do not justify the cost and risk to human life. By this account, you space miners, you builders of self-sustaining H3-extracting settlements on the moon, you Hiltons of space with your orbiting hostels, even you tourist promoters eyeing brief near-space junkets for the rich – all of you are promoting projects that are economically unprofitable, scientifically unjustified, and morally dubious.

No less a pundit than Neil deGrasse Tyson seems to have reached a similar conclusion. He argues that governments rather than private industry will have to sponsor the first human trips to Mars. Industry won't do it, Tyson says, because it will be hugely expensive, with high probability of fatalities and no economic return. If he means that only governments are misguided, lobby-ridden, and morally obtuse enough to engage in such activity, I agree. But even governments cannot escape the problem of moral hazard without some overwhelming purpose to justify the sacrifice of human lives that even the most optimistic admit will be required.

On this point, the MIT study purports to come to the rescue. If tangible benefits do not meet the moral hazard or even the economic test of human space flight, what does? Intangible benefits, of course – those which the Study disingenuously identifies as the "primary" goals of space travel. Why primary? Because the authors say so! The great benefit of intangible goals to any piece of advocacy – especially one written by scientists – is that they are not quantifiable. In the great scales of ethics and economics, they can have any value you choose to give them. Things you can

measure are recalcitrant; they don't yield to the political narrative. Intangible returns, on the other hand, can explain, balance, and justify anything. Chief among the intangible "primary goals" of human space exploration, the MIT study identifies "international prestige," and who can say they're wrong? Once intangibles enter the door, science flees out the window, and suddenly we are in a fantasy land of national narrative, quest sagas, and public relations – and never mind that Buzz Aldrin has taken to doing underwear commercials.

I'm not a scientist, but I am willing to trust the MIT investigators. I accept the idea there is no economic or scientific benefit in human space flight that will offset the cost in lives and treasure it involves. I would go further. Boosters have been overpromising the benefits of human space flight for fifty years, and it is past time to call their bluff. Where are the promised scientific achievements from human habitation of the space station? I can answer that question: always sometime just after the next budget cycle. What might have been done with the 120 billion dollars in construction costs for the space station, or with the 500 billion – at least – that another manned venture to the moon and Mars would cost? It would go a long way toward easing the budget squeeze on those charged with improving our nation's missile and space defenses, not to mention repair our rotting terrestrial infrastructure. I have to admit: as I contemplate NASA's heavy launcher to nowhere, and its silly plan to tether men to asteroids, I can't help thinking what building a more humane, more enlightened, better-paved, and better defended nation would do for our international prestige!

In short, human space exploration is a jobs program for the few, and an impediment to both national defense and the expansion of human knowledge. It might be thought of as the modern equivalent of flagpole sitting: once we put aside xenophobia and national exceptionalism, the only point seems to be to find out how long someone can stand it.* Even the nationalists and xenophobes are destined in the end to be disappointed. However specious the reasoning, our species will eventually send a few sacrificial humans to Mars. The first of them will step on *terra nova* long after I join the choir celestial; but it doesn't take a seer to predict that the flag she plants will not be that of any one nation but rather a pastel creation (think UN blue) representing a consortium of nations and industries and probably designed by Elon Musk, one of whose companies will have purchased all the film rights and logo space on the lander.

*For the record, the disputed record for flagpole sitting is 68 days, claimed by one John "Shipwreck" Kelly. The verified record for time in space is 438 days by the Russian Valeri Polyakov. Polyakov's record involved some trillions of dollars of infrastructure investment; Kelly required only a pole, a rope, two buckets, and an assistant whose name is lost to history.

Notes for Contributors to *Space & Defense*

Space & Defense seeks submissions that will contribute to the intellectual foundation for the integration of space policy into overall security studies. The collaboration of soldiers, scholars, and scientists studying nuclear deterrence in the 1950s led to a robust evolution of doctrine that shaped national and international policy for the succeeding forty years. Our goal as a Center is to create this same robust dialogue with a research agenda that focuses on the integration of space policy and security studies.

Indeed, the emergence of space as a unique and critical element in national security, economic security, homeland security, cyber security, environmental security, and even human security has persuaded us that this line of inquiry is vital to the future of international security.

Contributions are welcome from academic scholars and policy analysts at think tanks and research institutes; senior management and policy officials from international and governmental agencies and departments relevant to space and security issues; senior management and policy officials from organizations responsible for critical national and international infrastructures that rely upon space; major aerospace corporations; scientists and engineers interested or involved in space and security policy issues; military officers and operators in relevant units, commands, and in staff colleges and service academies.

The journal welcomes submissions of scholarly, independent research articles and viewpoint essays. There is no standard length for articles, but 7,500 to 10,000 words, including notes and references, is a useful target for research articles, and viewpoint essays should be in the range of 2,500 to 5,000 words. The opinions, conclusions, and recommendations expressed or implied within *Space & Defense* are those of the contributors and do not reflect those of the Eisenhower Center for Space and Defense Studies, the Air Force Academy, the Air Force, the Department of Defense, or any other agency of the United States Government.

Articles submitted to *Space & Defense* should be original contributions and not under consideration for any other publication at the same time. If another version of the article is under consideration by another publication, or will be published elsewhere in whatever format, authors should clearly indicate this at the time of submission. When appropriate, all articles are required to have a separate abstract of up to 250 words that describes the main arguments and conclusions of the article.

Details of the author's institutional affiliation, full address, and other contact information should be included in a separate file or cover sheet.

Contributors are required to submit all articles electronically by email attachment as a Microsoft word file (.doc or .docx format).

Contributors should not submit PDF files. All manuscripts submitted to *Space & Defense* need to be double-spaced with margins of 1inch or 2.5 cm, and all pages, including those containing only diagrams and tables, should be numbered consecutively. It is the author's responsibility to ensure when copyrighted materials are included in a manuscript that the appropriate copyright permission is received by the copyright holder.

Address manuscripts and all correspondence to:
Dr. Damon Coletta, Damon.Coletta@usafa.edu (e-mail),
or 719-333-8214.

On the basis of the peer reviews for research articles, the academic editors will make a final decision for publication. If required, the author(s) will be required to make additional changes and corrections as a result of the external peer review.

TABLES AND FIGURES

All maps, diagrams, charts, and graphs should be referred to as figures and consecutively numbered and given appropriate captions. Captions for each figure should be submitted on the same page as the figure to avoid confusion. Tables should be kept to a minimum and contain only essential data. Each figure and table must be given an Arabic numeral, followed by a heading, and be referred to in the text. Figures and tables are not to be embedded in the text. Each table and figure should be clearly labeled. In the text, make sure and clearly explain all aspects of any figures or tables used.

STYLE

Authors are responsible for ensuring that their manuscripts conform to the style of *Space & Defense*. The editors will not undertake retyping of manuscripts before publication. Please follow the Chicago Manual of Style.
Listed below are some additional style and writing guides:

- Dates in the form: 1 January 2009.
- Headings (bold, ALL CAPS, title case and centered).
- Subheadings (bold, italic, title case and centered).
- Acronyms/abbreviations should always be spelled out in full on first use in the text.
- The 24-hour clock is used for time, e.g., 0800, 1300, 1800.
- Use percent rather than % except in figures and tables.

• For numbers, spell out numbers less than 10.
• Make use of 21st style where appropriate
• Keep capitalization to a minimum.
• Concise paragraphs and sentences are desirable.
• Avoid a paper that is just descriptive; rather engage in analytical rigor and assessment.
• Avoid policy recommendations in the analysis part of paper; leave this, if applicable, for a separate section at the end of the paper.
• Define all new terms used in paper.
• Avoid hyphenated words when possible (e.g. low Earth orbit).
• Avoid the use of passive voice when possible.

FOOTNOTES

Footnotes need to be numbered consecutively with a raised numeral in the text. Please make use of the Insert-Preference-Footnote function of Word. Please do not use endnote style or scientific notation. Footnotes should be in full bibliographic style with first name, last name format for author.