Strategic Security: Toward an Integrated Nuclear, Space, and Cyber Policy Framework

Jason D. Wood[1]

This study documents the interaction of three vital elements of U.S. strategic security – the nuclear, cyber, and space domains. Demonstrating that these three domains overlap significantly in terms of function, technical capacities, and future challenges, it is argued that each should be integrated into an overarching policy approach that effectively coordinates U.S. nuclear, cyber, and space posture, capacities, and strategy.

Introduction

How do the nuclear, cyber, and space domains interact and what are the policy implications of these interactions going forward? This study argues that nuclear, cyber, and space capabilities are mutually reinforcing elements of U.S. strategic security in the 21st century, interacting significantly in terms of function, technical capacities, and future threats/challenges. Accordingly, each of these domains should be integrated into an overarching policy approach that effectively coordinates U.S. nuclear, cyber, and space posture, capacities, and strategy. While the Obama Administration has taken some positive steps to better coordinate nuclear, cyber and space policies, more can and must be done.

Why is this issue important?

Strategically speaking, the United States is in a period of transition. In the nuclear arena, the Obama Administration has articulated an ambitious agenda to recalibrate a Cold War nuclear arsenal to the modern security environment. First heralded in a now-canonical April 2009 speech in Prague, President Obama's agenda focuses on reducing the role of nuclear weapons in U.S. national security with the goal of

---

[1] Jason D. Wood is a Washington, D.C.-based Policy Analyst with Science Applications International Corporation. Working in support of the Defense Threat Reduction Agency's Advanced Systems and Concepts Office, his research focuses on nuclear deterrence, arms control, security assurances, fourth generation nuclear weapons, and deterring WMD terror attack. In 2010, Jason co-authored a case study on the legislative origins of the Nunn-Lugar Cooperative Threat Reduction Program, published by National Defense University's Center for the Study of Weapons of Mass Destruction. Previously, Wood was a Research Associate at the Institute for Foreign Policy Analysis, researching national security space issues and missile defense. He earned a Master of Science with distinction from Missouri State University's Graduate Department of Defense and Strategic Studies in 2007, where he served as an Earhart Foundation Fellow. His writing has also appeared in *Joint Force Quarterly*, *World Politics Review*, *Comparative Strategy*, and *National Journal*. The views expressed in this paper are the author's alone.

eventually moving toward global nuclear disarmament. [2] Heavily influenced by the Prague agenda, the 2010 Nuclear Posture Review (NPR) has since set the tone for a number of significant policy developments – including negotiation of the New START agreement with Russia, and deliberations at the 2010 Nonproliferation Treaty (NPT) Review Conference.

In the same timeframe, the United States has taken significant steps to address a new and challenging strategic domain – cyber. While the recent launch of U.S. Cyber Command and the release of the Cyberspace Policy Review are certainly significant steps toward developing effective cyber policies and capabilities, much remains to be done in the years ahead.[3] Perhaps most importantly, the work of developing an effective doctrine for offensive and defensive cyber operations is still in process.

The space domain is also evolving rapidly, in at least two respects. First, the number of actors in space is increasing. While Russia was historically the United States' primary competitor in space, China and India are rapidly developing capabilities that will allow them to utilize space for military and commercial gain. Additionally, Iran and North Korea continue to pursue ballistic missile and satellite launch capabilities. Whether or not these new actors will observe the traditional "rules of the road" that stabilized U.S.-Russia space-sharing is a matter of some concern. Second, the strategic importance of space to the United States is increasing exponentially, and has become a vital asset for net-centric U.S. forces. Taken together, space is an ever more crowded, essential domain for the United States – creating the possibility that an irresponsible act by one rogue actor could have a devastating impact on U.S. security. These shifting dynamics will necessarily impact policy – a reality that is noted in the recently released National Space Policy Report.

In this period of transition and evolving policy dynamics, when important decisions are being made on nuclear, cyber, and space policy, it is critically important that policymakers understand how developments and decisions in one domain could have a broader impact in other strategic domains. Failure to consider these interactions and develop an effectively integrated policy could have dire consequences for U.S. strategic security in the decades ahead.

Scope, Roadmap, and Definitions

The motivation behind this study is very specific and limited. The study will not recommend strategy or doctrine. Additionally, it does not focus on or recommend a specific set of capabilities or force structure for the nuclear, cyber, or space community. Rather, it will document the need for an integrated strategic security policy by highlighting areas of mutually supportive overlap, showing the current state-of-play in Washington, and highlighting possible approaches to better integrate nuclear, cyber, and space policy.

---

[2] Remarks by President Barack Obama (Hradcany Square, Prague, Czech Republic: April 5, 2009). http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered/.

[3] William J. Lynn III, "Introducing U.S. Cyber Command," *Wall Street Journal* (June 3, 2010).

Before proceeding further, it is also necessary to define two terms that are fundamental elements of the argument being made. Throughout this article, the term "strategic security" is used to encompass the combined security and freedom of action afforded by effective and integrated nuclear, cyber, and space capabilities and policy – that is to say, those capacities and policies that underwrite or otherwise enable the United States to pursue its grand strategy and protect its vital national interests over the long term. In this instance, strategic security contrasts with the much broader, colloquial term "national security," which can apply to a wider array of often more immediate geopolitical variables. Here the focus is intended to be more specific.

Next, the word "integrated" can mean many things to many people. In post-9/11 Washington, the need to integrate, cross-pollinate, or otherwise amalgamate policy and information has become an omnipresent mantra in Capitol Hill hearing rooms. While the need to integrate is often assumed in the public debate, what it means in practice is still a lingering question mark for many departments, agencies, commands, and offices. For this study, "integrated" does not mean keeping an office "in the loop" nor is it limited to a series of ad-hoc briefings or consultations between various stakeholders. Rather, integrated policy is the result of a joint collaborative process that actively seeks to leverage, coordinate, and complement one domain with another – applying ways and means to a strategic end – the essence of geopolitics and strategy.

How do the nuclear, cyber, and space domains interact?

To understand the need for an integrated and mutually supportive strategic policy, the interdependencies and linkages between the nuclear, cyber, and space domains must be clearly articulated. Indeed, were it not for these highly nuanced and significant interactions, integrated policy would not be necessary in the first place. To make the linkages between nuclear, cyber, and space more coherent and easily perceived, this study proposes a three-level framework: (1) areas of functional overlap; (2) shared technical capacities; and (3) common threats or challenges in the future security environment. What follows is not intended to be an exhaustive list of the interactions across the nuclear, cyber, and space domains. Rather, the framework below is simply intended as a constructive starting point from which policymakers, implementers, and technical experts can begin to consider their overlapping interests.

Areas of Functional Overlap

The first, and perhaps most obvious, interactions between the nuclear, cyber, and space domains occur on a functional level – where the functioning of systems in one domain enable the functioning of systems in another. These interactions are not insignificant. Particularly in the area of space support to the nuclear mission, cross-domain support is a vital element of mission success.

Space Support to the Nuclear Mission. The United States relies heavily on space systems to perform vital functions in support of the nuclear mission. For early warning, Defense Support Program (DSP) satellites – first deployed in the 1970s – have provided virtually uninterrupted early warning capability from geostationary

orbit using sensitive infrared sensors to detect heat from missile and booster plumes against Earth's background.[4] While the Cold War utility of DSP satellites is obvious, they continue to be vital in the detection of rogue state missile launches from Iran and North Korea. DSP satellites have also kept a watchful eye on modern intercontinental ballistic missile (ICBM) development in Russia and China and have been continually updated in the run-up to deployment of follow-on systems like the Space-Based Infrared System (SBIRS).[5]

To monitor force structure developments in other nuclear-weapon states (NWS) and possible proliferation activities in non-nuclear-weapon states (NNWS), U.S. space-based intelligence, surveillance and reconnaissance (ISR) capabilities provide vital intelligence that would otherwise be inaccessible to policymakers. Unlike modern unmanned aerial vehicles (UAVs) or manned platforms, space-based ISR assets "offer the benefit of global coverage, near invulnerability, and sustained operations over a continuous period of time."[6]

In addition to monitoring foreign military forces and nuclear proliferation, space-based ISR platforms play a key role in monitoring compliance with bilateral arms control agreements and form the backbone of "national technical means of verification" enshrined in formal treaty language. As the United States moves forward with President Obama's ambitious nuclear policy agenda, the need for space-based systems to monitor compliance with future initiatives – like the New START Treaty, the Comprehensive Test Ban Treaty (CTBT) and a Fissile Material Cut-Off Treaty (FMCT) – is already abundantly clear. In May 2010, the U.S. Air Force "launched the first of a number of satellites intended to monitor for signs of a nuclear test detonation."[7] This capability – and the level of verification, monitoring, and trust it stands to provide – may play a key role in garnering the political support necessary to conclude future arms control agreements.

Additionally, the communications capability provided by space-based systems like Milstar and the Defense Satellite Communications System (DSCS) is a key component of U.S. nuclear command and control – enabling secure, global communication between key military command nodes. More recently, the evolving, layered U.S. ballistic missile defense system (BMDS) relies heavily on space-based assets to detect and track enemy missiles. Finally, to the extent that conventional force components provide support to nuclear operations, it is important to note that space-based systems play a significant role in conventional military force enhancement, to include geodesy/earth observation, meteorology, communications, timing, and navigation.[8]

---

[4] *Space and U.S. Security: A Net Assessment* (Washington, DC: The Institute for Foreign Policy Analysis, January 2009): 8-9.
[5] Craig Covault, "DSP Satellites See Aggressive New Chinese Missile Testing," *Aviation Week & Space Technology* (April 8, 2007).
[6] *Space and U.S. Security: A Net Assessment*, 9.
[7] "Air Force Launches Satellite for Spotting Nuclear Tests," *Global Security Newswire* (June 1, 2010).
[8] See Peter L. Hays, *United States Military Space: Into the Twenty-First Century* (Maxwell AFB, AL: Air University Press, 2002).

The Functional Intersection of Space and Cyber. The similarities between the space and cyber domain are striking. Both are global – as opposed to territorial – domains, largely comprised of contested commons. Cyber and space share common networks, systems, and infrastructure. Additionally, both domains function primarily in a support role, providing the most vital and depended-upon capabilities for other domains (nuclear, air, land, and sea).[9] Given these similarities, it is not surprising that they play a closely related, mutually supportive role in U.S. strategic security.

Above all else, cyberspace is rooted in communication. Through the use of space-based systems, the United States can connect cyber environments anywhere on the planet. The primary benefit of connecting cyber domains through space is that it reduces the forward-deployed footprint of vital information resources. Absent the cyber connectivity provided through space, U.S. forces would not be able to rapidly aggregate large quantities of archived information – from imagery to battlefield intelligence.[10] Additionally, space enables cyber connectivity where fiber optic networks are not available or sufficient bandwidth is lacking.

Just as space supports the cyber domain, the reverse is true. As space grows ever more crowded and cyber capabilities proliferate, the need for encryption of satellite systems and communications has increased. Here, cyber plays a significant role in ensuring information security for satellite communications. For example, as noted during a recent session at the Air Force Association Global Warfare Symposium, "If you look at things like command and control, [or] on-orbit stationing of assets, you then have to look at the up-link, the down-link, and the ground control station, and then the various nodes that extend out from that…each one requires in-depth cyber protection. So they work hand in glove, you can't do one without the other… and when you combine things like offensive information [cyber] operations and strategic space intelligence assets, you can really tip the balance of power."[11]

The Cross-Cutting Reality of Cyber. Finally, it should be emphasized that the cyber domain permeates virtually every level of increasingly net-centric nuclear command and control and space capabilities. Thus, "[while] the cyber world is both separate from the domains of sea, air, space, and land [it is] ubiquitous throughout them. What this means is that cyberspace reaches across services, cultures, nations, and ideologies."[12] As one senior Department of Defense official recently noted, the

---

[9] Scott Cuthbertson, "Space: An Enabling Domain," Presentation to the Institute for Land Warfare Army Fires Symposium (Fort Worth, TX: July 21, 2010): 4.
[10] Craig Cooning, Speech to the Air Force Association Global Warfare Symposium "Integrating Space and Cyberspace Across Warfighting Domains," Defense Industry Panel (Los Angeles, CA: November 19, 2009).
[11] Lt. Gen. Brian Arnold, USAF (ret.), Speech to the Air Force Association Global Warfare Symposium "Integrating Space and Cyberspace Across Warfighting Domains," Defense Industry Panel (Los Angeles, CA: November 19, 2009).
[12] Nancy E. Brown, "Difficulties Encountered as We Evolve the Cyber Landscape for the Military," *High Frontier: The Journal for Space & Missile Professionals* Vol. 5 No. 3 (Air Force Space Command, 2009): 6. http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf.

functional role of cyber extends well beyond our nuclear and space forces: "Not only are our strategic forces, [and] our flow of conventional forces, dependent on cyber capabilities, but our society, our air traffic controllers, our financial networks, [and] our electric power grids. There are very few key elements of our society that are not potentially vulnerable to attack."[13]

Shared Technical Capacities

In addition to areas of functional overlap, the nuclear, cyber, and space domains share several technical capacities that enable the United States to field advanced systems in each domain. These include complex material and equipment manufacturing. Of particular importance to the space and nuclear domain is the ability of the United States to domestically design, engineer, and produce rocket propulsion systems – used in both space launch and ICBM systems.

Additionally, all three domains depend on a capacity to field secure, reliable, and highly advanced information technology systems. Across the nuclear, cyber, and space domain, the United States "must know the origin of the software and hardware in our computer systems and our satellites. It doesn't make much sense to have a computer system built with chips and run on software created in the country that is the most active cyber espionage adversary we face…Defense Department supply chains for computer systems and electronic components must come from trusted foundries and use trusted software. [U.S.] satellites should be remotely reprogrammable in the event of a cyber attack."[14]

Common Threats and Challenges in the Future Security Environment

In addition to functional overlap and shared technical capacities, the nuclear, cyber, and space domains face similar threats and challenges going forward. These shared threats and challenges reflect a cross-domain interest in developing innovative policy solutions going forward – solutions that recognize the broader scope of the threats/challenges and are integrated accordingly.

The Outside Cyber Threat to U.S. Nuclear, Cyber and Space Capabilities. As noted earlier, the cyber domain permeates virtually every aspect of U.S. nuclear and space capabilities and underpins the broader aspects of U.S. national security – to include the economy and civil infrastructure. This far-reaching network of interconnected systems and capabilities creates similarly far-reaching vulnerabilities to cyber attack from adversaries, including foreign governments, non-state actors, and commercial entities.

---

[13] Michael Nacht, Speech to the 38th IFPA-Fletcher Conference on National Security Strategy and Policy "Air, Space, and Cyberspace Power in the 21st Century," (Washington, DC: January 20, 2010).

[14] Larry Wertzel and Randy Forbes, "Bolster U.S. Cyber Defenses: Make Comprehensive Push Against Global Threats," *Defense News* (31 May 2010).

For example, "the command and control networks used to control nuclear weapons might be targets of cyber attack." [15] According to a recent report from the International Commission on Nuclear Nonproliferation and Disarmament (ICNND), "nuclear command and control has inherent weaknesses in relation to cyber warfare." During the Cold War, mutually assured destruction required that a targeted state be able to launch a retaliatory strike very quickly – to assure the destruction of its adversary and thus eliminate any first-strike incentive. The ability to mount a devastating response to a first-strike necessarily compressed decision timelines associated with a nuclear launch order. On the other side of the equation, the need to assure an adversary of a second-strike capability following a retaliatory strike created the need for survivable nuclear forces spread out over a wide geographic area. [16]

In the post-Cold War, cyber era, widely dispersed, legacy nuclear command and control systems provide ample entry points for exploitation through cyber attack. Abbreviated decision timelines make it easier for terrorists to spoof an attack and provoke a devastating response because very little time or debate is afforded to assess the situation in full. As the ICNND report argues, "These rapid response times don't leave room for error. Cyber terrorists would not need deception that could stand up over time; they would only need to be believable for the first 15 minutes or so."[17]

Additionally, the need to reduce the time it takes to disseminate plans and orders to nuclear forces has likely expanded the use of computers in nuclear command and control. In recent years, the United States has worked to integrate traditional nuclear command and control (C^2) into the broader architecture now referred to as command, control, *computers*, communications, intelligence, surveillance, and reconnaissance (C^4ISR), further hinting at increased reliance on cyber systems throughout the strategic architecture.[18]

In the space domain, "One might, for example, jam [a satellite] command uplink so that it cannot receive commands from the ground. In the absence of such commands, a satellite might not be able to execute a given mission or it might drift out of position. A satellite may use an unencrypted command link, so that an adversary could manipulate the satellite's functions."[19] A cyber attack on U.S. command and control nodes that exploits rapid decision timelines and increased

---

[15] William Owens, Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press): 296-297.

[16] Jason Fritz, "Hacking Nuclear Command and Control," (Barton, Australia: International Commission on Nuclear Nonproliferation and Disarmament, 2009): 8. For an overview of U.S. nuclear command and control systems, see Robert D. Critchlow, "Nuclear Command and Control: Programs and Issues," (Washington, DC: CRS Report to Congress, May 3, 2006).

[17] Ibid, 8-11.

[18] Ibid. The need to assure rapid retaliation did lead to the introduction of autonomous, computer-controlled nuclear launch systems during the Cold War. See David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* (New York, NY: Doubleday, 2009).

[19] Owens, *Technology, Policy, Law and Ethics*, 297.

reliance on computers, mounted in coordination with a cyber attack on space-based elements of the strategic architecture could severely compromise U.S. strategic security in a matter of minutes.

Control of Dual-Use Technologies and Intellectual Property Across Domains. Aside from the cross-cutting cyber threat to U.S. strategic capabilities, all three domains are currently challenged by a growing commercial/non-state presence that has the potential to create vulnerabilities and proliferate dangerous dual-use technologies and sensitive intellectual property.

By the mid-1990s, global commercial revenues from space were greater than the aggregate of all government spending on space. In 2007 alone, "spending on commercial space infrastructure, infrastructure support industries, and commercial satellite services totaled approximately $174 billion, accounting for nearly 70 percent of total global space spending."[20] The commercial utilization of space creates the possibility that sensitive technologies used in satellite manufacturing, launch, and satellite services will proliferate beyond U.S. borders, shortening the path to advanced capabilities for states like Iran, North Korea, China and India. The same can be said in the nuclear and cyber domains, where the global expansion of civil nuclear power and information technology has increased the commercial/non-state presence in key strategic domains. This is particularly worrisome given the proven ability of illicit trafficking networks to supply terrorists with weapons of mass destruction (WMD)-related information and technology.

These threats will require the United States to pursue effective, integrated policies to control sensitive technology and information across the nuclear, cyber, and space domains – where vulnerabilities in one domain can easily transfer across overlapping functional and technical boundaries. Indeed, it is not sufficient to have airtight control over nuclear technology exports alone, if cyber vulnerabilities and poor control over space technology affords adversaries a wide-open backdoor to cripple U.S. nuclear command and control. In this sense, cyber is a glaring vulnerability that could easily lead to compromised capabilities in the nuclear and space domain. While the United States does have an extensive export control regime in place to prevent the sale of sensitive information and technology overseas, these regulations are not capable of preventing scores of cyber intrusions that could potentially threaten U.S. national security.[21]

Deteriorating Industrial Base. In addition to the challenges of dual-use technology and growing commercialization across all three domains, the United States is grappling with a deteriorating industrial base and workforce across the space and nuclear domains. As with functional overlap and shared technical capacities, these deficiencies have the potential to spill over across domains.

For example, NASA is preparing to retire the Shuttle Transport System (STS) in early 2011, and plans to depend on future commercial systems for manned

---

[20] *Space and U.S. Security: A Net Assessment*, 11.
[21] For more on the challenges of cyber security, see *Securing Cyberspace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, December 2008).

spaceflight, using Russian platforms in the interim. At the same time, the U.S. commercial launch industry has struggled to compete with international launch service providers, many of whom are heavily subsidized by national governments. Indeed, the U.S. share of global launch industry revenue has continually declined, with U.S. providers owning 37 percent of revenue in 2006, compared with 50 percent in 2005 and a high of 66 percent in 2003.[22] Thus, NASA appears to be pinning its future manned launch capability on a commercial industry that is poorly positioned to rapidly deploy a follow-on to the space shuttle. In the time between retiring STS and producing a U.S. commercial follow-on, the United States will effectively subsidize a generation of Russian rocket engineers. Meanwhile, absent the STS, an as-yet irreplaceable generation of U.S. rocket scientist will likely retire in obscurity.

While the United States can surely survive without a manned spaceflight capability in the short term, there is little doubt that the United States will at some point require a new generation of ICBMs to support a robust nuclear deterrent. Here, the workforce and infrastructure challenges of space intersect with the nuclear domain. Who will design the solid-fueled rocket motors required to boost ICBMs and their sea-launched counterparts over the long term? In that endeavor, the Russians cannot assist and U.S. commercial industry could be ill-staffed to provide systems that have not been built at home in more than a generation.

Similar infrastructure and workforce dynamics are playing out in other areas – where dwindling expertise lengthens the timelines associated with developing new satellite systems, and national laboratories struggle to recruit the next generation of nuclear scientists absent a clearly defined plan of modernization and development. Given the potential for these shortcomings to have effects across three strategically important domains – nuclear, space, and cyber – U.S. policymakers must seek to develop innovative policy remedies that fully incorporate the workforce and infrastructure challenges of all three areas. Indeed, a laboratory capable of producing modern nuclear weapons is of little utility without a cadre of rocket engineers to produce delivery vehicles and the satellites to guide them.

What is the current state-of-play?

As noted in the introduction, the Obama Administration has taken some positive steps to integrate nuclear, space and cyber policy under the umbrella of strategic security. Early in 2009, Under Secretary of Defense for Policy Michèle Flournoy established a new office in the Pentagon, that of the Assistant Secretary of Defense for Global Strategic Affairs (GSA), then headed by Dr. Michael Nacht. According to the Department of Defense (DOD), GSA "is a newly configured directorate in the Office of the Secretary of Defense (OSD) that develops policy for the Secretary on countering weapons of mass destruction, nuclear forces and missile defense, cyber security and space issues."[23] Whereas previous administrations maintained separate organizations for nuclear, cyber, and space policy, the Obama administration noted that each of these areas must be aggregated into one overarching approach that

[22] *Space and U.S. Security: A Net Assessment*, 15.
[23] See http://policy.defense.gov/gsa/index.aspx.

connects threats, technologies, and capabilities from each domain, supporting overall U.S. strategic security.

Under the umbrella of GSA, DOD recently conducted three important posture reviews – the NPR, the Ballistic Missile Defense Review (BMDR), and the Space Posture Review (now referred to as the National Space Policy Report). However, aside from policymaker assurances that the reviews involved a wide array of stakeholders and were "sufficiently cross-pollinated," there are few indications that these reviews were fundamentally integrated to account for the significant functional, technical, and threat-based overlap across domains. Perhaps more importantly, there is no formal mechanism in place to oversee the long-term implementation and integration of these policy reviews.

Of the policy domains under GSA's purview, cyber is the newest and perhaps most challenging. In the nearly two decades since the rise of the information age, a unified theory of cyber deterrence and cyber warfare has remained elusive throughout the U.S. government and DOD. Not surprisingly, "this lack of a government wide cyber doctrine creates a potential for inadequate and ineffective responses to cyber threats…the current doctrine lacks adequate interoperability principles to govern a joint cyber force."[24]

As noted earlier in the introduction, DOD recently established U.S. Cyber Command to take the lead on cyber issues with the department. However, this was not accomplished without some controversy regarding the structure, mission, and leadership of the new command – largely a reflection of the lingering confusion surrounding the cyber domain as a whole.[25] Whether or not Cyber Command will be a turning point for U.S. cyber efforts remains uncertain. What is clear is that "without a properly coordinated doctrine, the Cyber Command's capabilities might first be tested during an actual national emergency. Such a crisis may highlight the inadequacy of the command's organizational structure, gaps in its roles and missions, or insufficient intelligence authorities."[26]

Given the strategic scale of the cyber threat, it is perhaps tempting to apply the rich theoretical foundations of nuclear strategy/deterrence to the cyber domain. While this study argues for integration of policies across strategic domains, integration should not be conflated with substitution or mirror-imaging. Just the opposite, there are unique challenges in the cyber domain to which nuclear deterrence theory is ill-suited. In the process of developing an effective cyber doctrine/policy that recognizes the functional, technical, and threat overlap among nuclear, cyber, and space, the United States should not assume that the lessons of Cold War deterrence are an adequate framework for policy in the cyber domain.[27]

---

[24] Mark D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law & Policy* Vol. 4 (2010): 180.
[25] Eric Sterner, "Re-Categorizing Cyber Conflict," *World Politics Review* (July 8, 2010).
[26] Ibid, 181.
[27] Owens, et al. *Technology, Policy, Law, and Ethics*, 293-297. See also John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York*

Thus, overall, the current state-of-play is insufficient. Though the move to create an office within DOD responsible for strategic policy is worthwhile, more can be done to coordinate policy reviews conducted under GSA – with special attention given to formal implementation mechanisms. Similarly, the establishment of U.S. Cyber Command signals that DOD, and the U.S. government as a whole, recognizes the scope and seriousness of the cyber threat. However, efforts to develop a minimally adequate – much less cross-domain integrated – doctrine/policy have fallen short.

Problems Extend Beyond Policy to Acquisitions

Alongside the need to better integrate policy in the nuclear, cyber, and space domains, it is also important to closely integrate and coordinate the acquisition of vital components that support capabilities across all three domains.

One area where this synchronization is clearly lacking is space support to the nuclear mission. Nearly a decade ago, the U.S. Air Force began development of the Family of Aerial Beyond-line-of-sight Terminals (FAB-T) to connect U.S. strategic nuclear bombers with the forthcoming Advanced Extremely High Frequency (AEHF) system, the next generation of nuclear command and control satellites. As detailed in a recent command and control trade journal, "in a nuclear war, ground antennas would be knocked out, the U.S. president would take to the air in a mobile command post (E-4B), and FAB-T computers on the bombers would become the president's last link to the bombers." Currently, the president does not have that type of air-to-air satellite link, because U.S. strategic bombers do not carry Milstar terminals – the forerunner to AEHF.[28]

However, with the first AEFH satellite slated to launch in September 2010, there is a major delay in fielding FAB-T. "Development of the terminals is years behind schedule and the Air Force will not decide until 2010 whether to begin production."[29] While AEHF is scheduled to achieve initial operating capability in 2011, a recent Government Accountability Office report estimates that "FAB-T will not have all of its terminals fielded until fiscal year 2019."[30] Thus, while an on-orbit system is mission-ready, the subsystems needed to extend this capability to another domain are not keeping pace.

What should be done to better integrate nuclear, cyber, and space policy?

The significant overlap between the nuclear, cyber, and space domains demands that government leaders adopt innovative, purposeful, and formal approaches to integrating policy across all three domains. While the future challenges posed by

---

Times (January 26, 2010) and Joshua Pollack, "Is the Cyber Threat a Weapon of Mass Destruction?" *Bulletin of the Atomic Scientists* (January 20, 2010).

[28] Jim Hodges, "Out of Sync: U.S. Air Force Copes with Delays on Nuclear Control Terminals for Bombers," *C4ISR Journal* (July 2010): 28-29.

[29] Ibid.

[30] "Challenges in Aligning Space System Components," (Washington, DC: U.S. Government Accountability Office, October 2009): 9.

nuclear proliferation, cyber attack, and a crowded space domain are unique in history, the past does provide useful guidance on how to better integrate and align policy across a variety of stakeholders.

The Nuclear Weapons Council as a Template for Policy Integration. During the Cold War, policymakers faced a number of difficult, widely scoped policy problems in a new and important domain of warfare – nuclear. Though the challenges facing today's policymakers are unique both substantively and contextually, the past does offer some instructive lessons that can be applied to integrating policy across strategic domains.

Seeking to maintain civilian control over the use of nuclear energy and the stewardship of nuclear weapons, the 1946 Atomic Energy Act created the Atomic Energy Commission (AEC). The Act also established the Military Liaison Committee (MLC) – intended to provide a voice for the military at the AEC. However, by the late-1970s, the AEC had evolved into Department of Energy (DOE) and the original impetus behind the MLC – an intra-agency group within DOD, not an interagency organization – had become obsolete as a result. Additionally, the cost of funding the U.S. nuclear weapons program across two departments –DOD and DOE – was of growing concern to several members of Congress. To examine these issues and identify a way forward that balanced civilian control of nuclear weapons with the need for DOD input – while effectively managing cost and other programmatic issues – the National Defense Authorization Act for Fiscal Year 1985 directed President Regan to establish a Blue Ribbon Task Group on Nuclear Weapons Program Management.[31]

Issuing a final report in July 1985, the Task Group identified several areas for improvement "intended to result in a closer integration between nuclear weapons programs and national security planning without sacrificing the healthy autonomy of [DOD and DOE] in the performance of their respective missions." Specifically, the Group noted the lack of a high-level, joint DOD and DOE body to coordinate nuclear weapons program activities. Absent the AEC, the staff and stature of the MLC had eroded to the point of irrelevance. As a result, the Task Group recommended establishing a senior-level, joint DOD-DOE group to coordinate nuclear weapons acquisition issues and related matters – the Nuclear Weapons Council (NWC).[32]

Today, the jointly staffed NWC – located within the Acquisition, Technology, and Logistics (AT&L) structure at DOD – serves as a high-level focal point for activities to maintain the U.S. nuclear weapons stockpile (see Figure 1, below). The Council provides an interagency forum for reaching consensus and establishing priorities between DOE and DOD. It also provides policy guidance and oversight of the nuclear stockpile management process to ensure high confidence in the safety, security, reliability and performance of U.S. nuclear weapons. The NWC meets regularly to raise and resolve issues between DOD and the National Nuclear Security Administration (NNSA) regarding concerns and strategies for stockpile

---

[31] *Nuclear Matters: A Practical Guide* (Washington, DC: Office of the Deputy Assistant to the Secretary of Defense – Nuclear Matters, 2008): 87-90.
[32] Ibid, 89-90.

management. The Council is also responsible for a number of annual reports that focus senior-level attention on important nuclear weapons issues. Significantly, "the original 1987 statute establishing the NWC and delineating its responsibilities reflected the concerns of the day…[and] has been amended several times. Each additional responsibility assigned to the Council has reflected emerging concerns as the Cold War ended and the post-Cold War era began."[33]

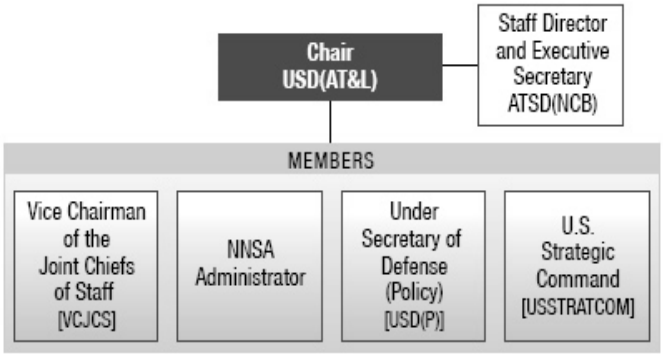

Figure 1. NWC membership. Source: Nuclear Matters: A Practical Guide.

As noted in the previous section, the Obama Administration has taken several positive steps to begin the integration of nuclear, cyber, and space policy into a unified policy framework for strategic security. However, the creation of GSA alone will likely prove insufficient for the coordination of strategic policy within DOD, let alone across the broader field of stakeholders throughout the U.S. government. This is especially true over the long term, given the propensity of incoming administrations to re-align the organization of politically appointed offices in order to reflect new priorities.

Going forward, beyond 2012, U.S. strategic security could be better served by a nuclear, cyber, and space policy framework that resembles the NWC more closely than the current organization under GSA. Specifically, a Strategic Security Council would have a legislative mandate that included specific authorities, roles, and responsibilities for integrating nuclear, cyber, and space policy across the broader national security community. Additionally, a permanent, formal organization resembling the NWC would have the benefit of dedicated interagency staff and subordinate action officer groups to prepare issues for high-level consideration. Significantly, a Strategic Security Council would own responsibility for producing regular, integrated reviews of U.S. strategic posture across all three domains and overseeing their implementation. Most importantly, adapting the NWC model to the task of integrating nuclear, cyber, and space policy would provide a formal mechanism for a process that is currently ad-hoc.

[33] Ibid, 87-90.

Concluding Thoughts

Clearly, nuclear, cyber, and space capabilities are mutually reinforcing elements of U.S. strategic security, overlapping significantly in terms of function, technical capacities, and future threats/challenges. Importantly, these fundamental elements of U.S. strategic security are rapidly evolving. In the nuclear realm, the United States faces possible proliferation among rogue states, terrorist acquisition of nuclear weapons, and a host of difficult policy challenges associated with implementing President Obama's nuclear agenda. Threats in the cyber domain are emerging more rapidly than solutions, while U.S. dependency on cyber capacities grows every day. In space, an increasing number of state and commercial actors will continue to exert pressure on a policy framework that was first developed a generation ago to accommodate the United States, Russia, and few others.

The significant cross-domain interactions – coupled with the rapidly changing strategic environment – demand that the United States develop policies that reflect and complement the shared roles, resources, and risks facing the nuclear, cyber, and space domains. Awareness of the need for better strategic policy integration is increasing throughout the national security community, as reflected in the recent establishment of GSA. However, more can and must be done, starting with a legislative mandate to establish a formal mechanism within DOD for nuclear, cyber, and space policy integration modeled after the Nuclear Weapons Council.

While the recent release of the Nuclear Posture Review, the National Space Policy Review, and the Cyberspace Policy Review are not insignificant – the most difficult work of developing and implementing an integrated strategic policy lies ahead. Where ad hoc mechanisms for policy integration and implementation fall short, a more formal and sustainable approach to U.S. strategic security policy can help ensure proper synchronization of roles, resources, and risk over the long term.