Non-Traditional Security Threats and Asia-Pacific Regional Cooperation

James M. Keagle, PhD

Center for Technology and National Security Policy
National Defense University

August 2012

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Non-Traditional Security Threats and Asia-Pacific Regional Cooperation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,300 5th Avenue SW Ft. Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**18**	

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, Department of Defense, or U.S. Government. All information and sources for this paper were drawn from unclassified materials.

James M. Keagle, PhD

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

James M. Keagle, PhD

Dr. James M. Keagle is the Director of the Transforming National Security seminar series at the Center for Technology and National Security Policy at the National Defense University (effective September 2007). Prior to this position, Dr. Keagle was the National Defense University's Provost (effective 2004) and Vice President for Academic Affairs (effective 2000). Prior to these positions, he served as a professor of National Security Strategy at NDU. In that role Dr. Keagle worked as a research faculty member assisting with NDU's modeling and simulation and work with interagency education and training.

Accepting an appointment to the U.S. Air Force Academy, he graduated second academically in his class in June 1974. Following graduation, he went to the University of Pittsburgh to complete his Master's of Arts degree in political science and earned a graduate certificate in Latin American studies. After a tour as a munitions maintenance officer, Dr. Keagle went on to become an assistant professor of political science at the U.S. Air Force Academy. In 1980, he went on to Princeton University where he completed both a Master's of Arts degree and Ph.D. in politics. He proudly notes his honorary PhD from the Military Technical Academy of Romania--the only United States citizen so honored.

Following his extensive education, Dr. Keagle's next six tours were political-military assignment that included direct access and interaction with Cabinet-level government officials on national security related matters. These assignments included work for two Combatant Commanders as a senior strategist; for the Office of Secretary of Defense pertaining to Cuba; Deputy Director, Office of the Secretary of Defense Bosnian Task Force; and for the Deputy Under Secretary of the Air Force in International Affairs as Senior Strategist. Military medals include the Defense Superior Service Award, the Legion of Merit, and the Purple Heart.

Concurrent with, and since leaving military service, Dr. Keagle has held the position of adjunct professor at a number of institutions to include: Syracuse University, American University, Central Michigan University, Catholic University, University of Colorado, and Lake Superior State College. He also holds honorary professorships with Transylvania University in Brasov, Romania, as well as the Mongolian Defense University--again, the only American so honored.

Contents

LIST OF FIGURES

INTRODUCTION

The *global commons* have routinely been considered as physical spaces that are not under direct nation-state control—common grassland that all must share, for example. They demand responsible management so as not to exhaust their supply (fisheries) or do irreparable harm to the world's ecosystem (species extinction, pollution of the atmosphere, contamination of potable water supplies). These spaces may also be vital to states and other global actors as they provide access and connectivity to the rest of the world (sea lines of communication). The global commons in the 21st century lexicon of security has expanded even further to consist of outer space, international waters and airspace, and cyberspace. Together the aforementioned constructs "constitutes the fabric or connective tissue of the international system," as Flournoy and Brimley noted in 2009.[1] Strategist Alfred Thayer Mahan used the term in describing the world's oceans as "a great highway… a wide common" in his 1890 volume, *The Influence of Sea Power Upon History*. Mahan's viewpoints influenced security policies and military capabilities for decades.[2] Today, as we push the envelope even further regarding our understanding and importance of the global commons, some suggest that the human species itself constitutes an essential element of the global commons and that human rights, equitable development, ethnic cleansing, and civil wars are legitimate parts of the expanding definition of the global commons. Regardless, the global commons is an important part of regional and global security and offers challenges and opportunities for cooperation as we share this planet.

Access to and use of the commons for political, economic, and military purposes has, until very recently, been almost an international fact of life. Nation-states have long utilized the commons to promote political ideals by using the open seas, and later airways, to diplomatically engage others around the globe. Economically, the "free" commons have contributed to globalization and the exploitation of the world's resources, providing a conduit to unite consumers with regional markets and marketers. Furthermore, nearly uncontested freedom to operate on the seas, in the air, in orbit, and in cyberspace meant that the United States and its allies exercised a high level of strategic freedom of maneuver as they focused on the prosecution of land and air campaigns around the world. This reality is changing rapidly as concerns about climate change and diminishing supplies of raw materials as well as the assertions about the rights of the oppressed (think Arab Spring) grow. Unlimited freedom to access and use the commons can and should no longer be taken for granted. Real and perceived scarcity must be addressed—not through conflict but rather through global and regional efforts to manage our planet and govern its inhabitants more responsibly. Better understanding of these security challenges and opportunities for expanded cooperation is the purpose of this paper.

[1] Michele Flournoy and Shawn Brimley, "The Contested Commons," *U.S. Naval Institute Proceedings* (July 2009): 17.

[2] Alfred Thayer Mahan, "The Influence of Sea Power Upon History," in *Roots of Strategy: Book 4*, ed. David Jablonsky (Mechanicsburg, Penn: Stockpole Books, 1999): [page 3].

THE GLOBAL COMMONS UNDER SIEGE

Three features of the current and expected operational landscape are most pressing, as noted in the 2010 U.S. *Quadrennial Defense Review*:

- Hybrid Threats that blur traditional categories of conflict
- Assured access to and stability in the Global Commons
- Frequency and severity of problems with chronically fragile states[3]

Each of these deserves serious explanation and study.

The Hybrid Threat

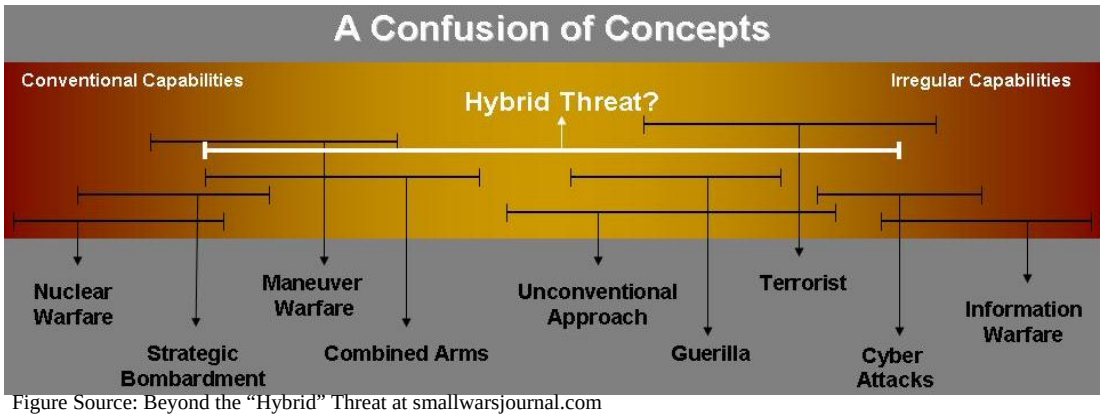

Figure Source: Beyond the "Hybrid" Threat at smallwarsjournal.com

Figure 1. The Hybrid Threat

- Adversaries are likely to seize the initiative and employ a mix of conventional weapons, irregular tactics, weapons of mass destruction, terrorism, cyber attack, and criminal behavior, supported by an information campaign
- Higher and lower intensity forms of conflict often converge, blurring the categories and features of warfare
- State or non-state actors (or combination thereof) employ a blend of two or more components of the spectrum of conflict, including economic, diplomatic, informational, and or/social domains

The 21st century is filled with examples of this type of conflict. Among those that come to mind are the Hezbollah efforts in Lebanon in 2006 and the array of Arab Spring movements in the greater Middle East beginning in 2011.

This more complicated threat environment is captured in the next several illustrations.

[3] *Quadrennial Defense Review*, Title 10, *U.S. Code*, Subtitle A, Pt. I, Chapter 2, §118 (b) (1), 1 February 2010.

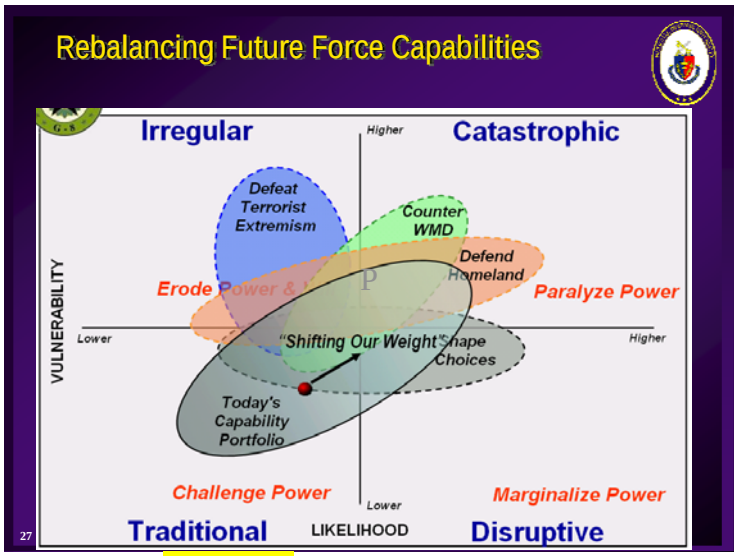

Figure 2. Shifting Our Weight

In Figure 2 the central message is that force capabilities must adjust to meet new security challenges. As we shift up and to the right, the role of large conventional forces engaging one another diminishes and new requirements emerge. These new security challenges provide opportunities for collaboration and cooperation—as well as posing non-traditional threats to security establishments.

It is likely to mean smaller conventional forces and greater attention to special operation forces, intelligence collection, and unmanned systems.

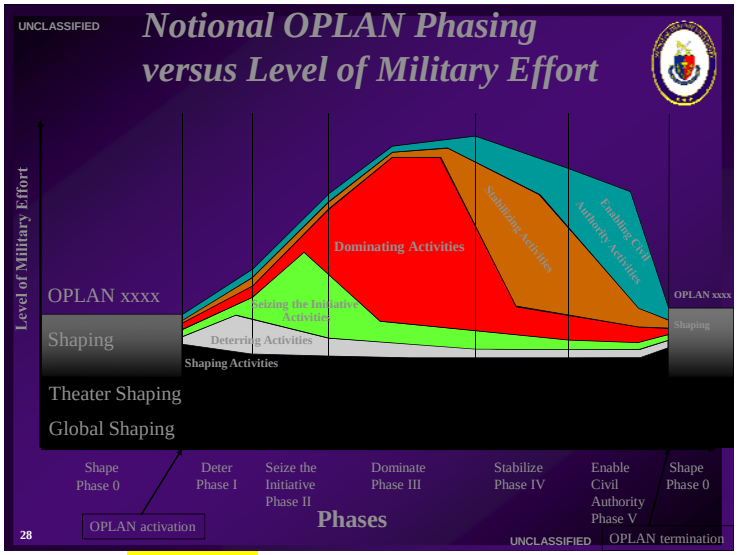

Figure 3. Notional OPLAN Phasing

Figure 3 even more dramatically tells the new story that avoiding war (Phase 0) is just as or more important than waging war or combat.[4]

[4] National Security Strategy 2010, The White House, May 2010

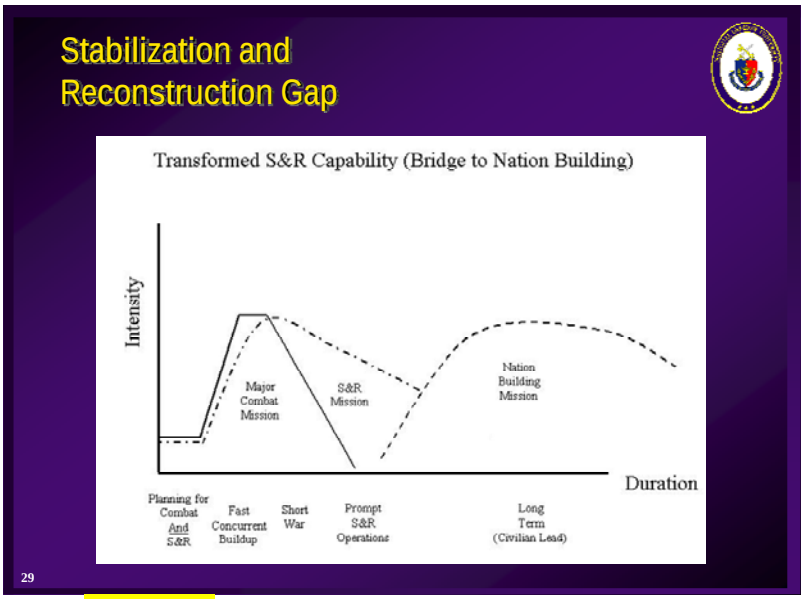

Figure 4. Stability and Reconstruction Mission

Figure 4 paints another powerful dynamic—that stability and reconstruction missions are now co-equal with major combat missions in terms of priority and importance.[5]

ACCESS AND STABILITY IN THE GLOBAL COMMONS

Perhaps the most pressing issue in the Asia–Pacific region is the PRC's anti-access/area denial strategy. The People's Republic of China (PRC) has leveraged military modernization programs combined with forward positioning of anti-ship ballistic missiles and economic and diplomatic policies into a position of greater influence. Arguably, by posing a greater threat not only to Taiwan but also to the U.S. Navy carrier battle groups, the PRC is causing other Asia-Pacific nations to reconsider their longer term political and military strategic alliances. The United States, for one, has announced the now oft-repeated pivot toward Asia—and taken steps to strengthen military and political ties with nations constituting the 2nd island ring around China—much like its containment strategy against the U.S.S.R during the Cold War. How all this plays out in the coming decades will largely shape the balance between conflict and cooperation in the region. Whether China is able to leverage the Shanghai Cooperation Council and other regional forums into effective tools of its long-term strategy of influence remains to be seen.[6]

The PRC has sought to wield this regional and global influence in the Arctic as well, as climate change begins to open up the Northern Route as a potential game changer in the distribution of fossil fuel resources from supply locations to countries that are dependent on external sources for their energy needs. As the maps in Figure 5 and Figure 6 highlight, Russian territorial claims in the Arctic assert sovereignty over a potential fossil fuel transportation route game changer. This becomes more than just a race to secure fossil fuel resources in the Arctic. The greatly reduced

[5] Joint Chiefs of Staff. *The National Military Strategy of the United States of America.* (Washington, DC, 2011)

[6] http://www.defense.gov/news/d20110714cyber.pdf Department of Defense Strategy for Operating in Cyberspace July 2011, as available on Internet May 29, 2012

shipping distances via a route that hugs the Siberian coast (and may be under Russian control) may fundamentally diminish the value of the Malacca Straits and other key transportation networks that currently serve the world's commerce. The United Nations convention on the Law of the Sea may prove insufficient to address these emerging issues.

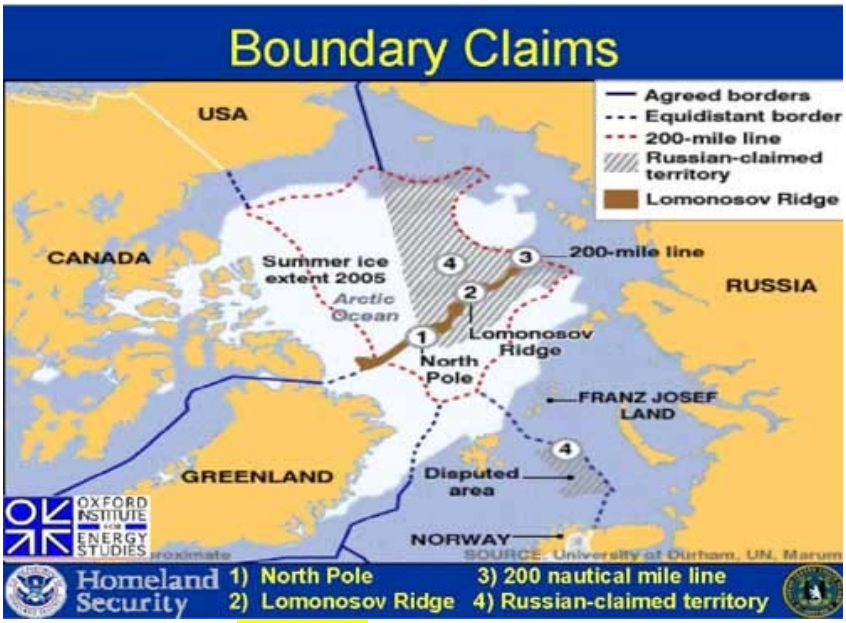

Figure 5. Boundary Claims

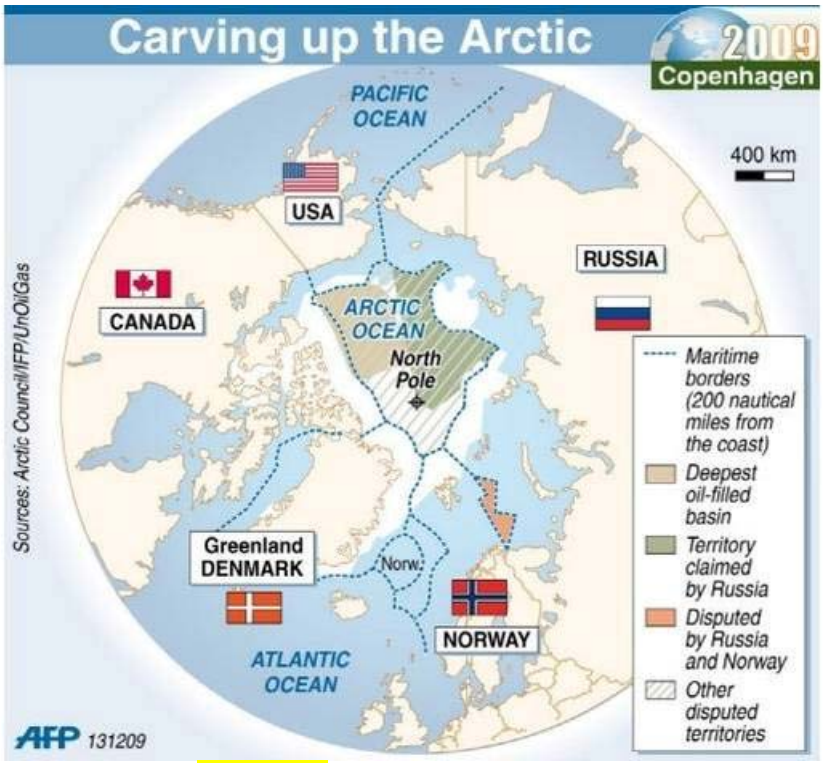

Figure 6. Carving up the Arctic

CHRONICALLY FRAGILE STATES

U.S. strategy has long concerned itself with economically and politically fragile states. Greater emphasis has been placed on this since the early days of the war on terror.

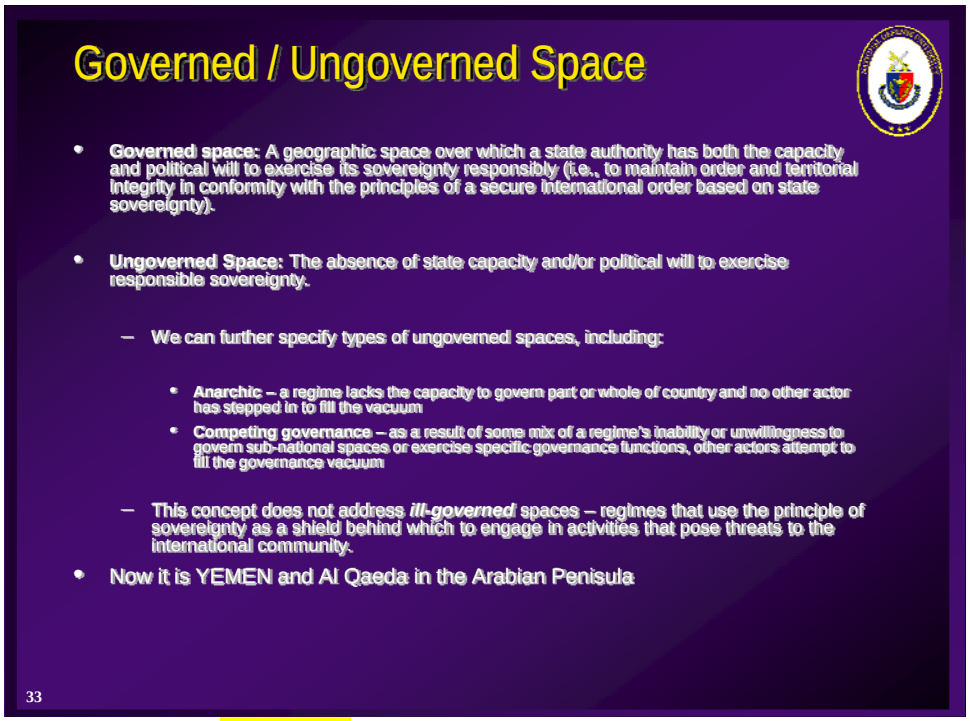

Figure 7. Governed/Ungoverned Space

Since 9/11 the language has included ungovernable or ungoverned spaces—where the host government lacks the physical capacity and/or the political will to exercise sovereign power. Within counterterrorism and counterinsurgency strategies, these areas have become breeding grounds and sanctuaries for terrorist organizations to operate and conduct operations with impunity. What followed are capacity development programs to defeat, deter, and dismantle these organizations. Both in terms of governance capacity and political will, as Figure 8 suggests, international cooperation will be key.

Figure 8. Capacity and Will

Whether best understood as nation building, stability and reconstruction operations, or long–term economic development, these will pose security challenges and opportunities for cooperation for the foreseeable future. It also raises the very difficult challenge of discriminating between civil wars, wars of external aggression, and genocide. The world has taken a clear position on genocide—Never Again. Yet it remains extremely difficult to obtain consensus for collective action in these cases, however clear the facts on the ground may seem to some. As the world wrestles with a period of tight and austere budgets, finding the funds for long-term socio-political and economic development and war avoidance strategies will be difficult.

While not limited to fragile states, humanitarian assistance and disaster relief (HADR) constitutes a fertile ground for regional cooperation. Be it in response to the 2011 earthquake off the coast of Japan and subsequent tsunami and nuclear reactor breaches or the tsunami that devastated Indonesia in 2008, HADR will be an essential element of the world's collective response to tragic natural events. The Transformative Innovation for Development and Emergency Support (TIDES) program shows initial promise for such collaboration. Its goals include leveraging global talent, integrating multiple approaches, and sustaining longer term development through private sector investment. It supports the basic needs of stressed populations by focusing on key infrastructures—water, power, shelter, cooking, cooling and heating, lighting, sanitation, and information and communications technology. TIDES goes beyond HADR to broader support for civil authorities and building their general capacities.[7]

[7] See www.star-tides.net for a more complete description of the TIDES program.

THE CHALLENGE OF THE GLOBAL COMMONS

Whether understood as air, land, sea, cyber, or space, these domains of the global commons comprise the infrastructure on which the global system operates and its major components flow—be it information, people, commerce, finance, technology, or military muscle. Individual, national, and global prosperity and governance depend on this interconnected and interdependent network of relationships that operate within and across these domains. Prosperity and freedom can be enhanced or threatened depending on how security challenges and regional cooperation efforts are balanced.

Outer Space

Society has become dependent on capabilities and information delivered to, from, and through space. Perhaps the most dramatic of these examples is the prosecution of the war against Al Qaeda. While some of the operational details remain unknown to the general public, it is commonly understood that the combination of special operations forces and intelligence officers rely on outer space to transmit data in almost real time regarding the location of individual human targets and the subsequent application of lethal force (via drones) across international air space and sovereign borders. This new kind of warfare may define conflict for the next several decades.

Furthermore, resourceful adversaries may leverage asymmetric technologies and unconventional approaches to circumvent traditional advantages, negate core strengths, and exploit vulnerabilities of competing forces. They could exploit the Outer Space Commons in a variety of challenging ways:

- Offensive computer network operations and electronic warfare with kinetic first strikes could disrupt battlefield network information and space systems.
- Space systems could deny the use of reconnaissance, early-warning, communications, navigation, and weather satellite assets that enhance land-based military operations.

Equally important, we have become highly dependent on space for more routine communications, be it the use of GPS for everyday mundane transport of goods, people, and service from one location to another, or the transmission of more secure information that is the lifeblood of international financial markets. Figuring out the rules and codes of conduct that should govern this domain is both a commercial and governmental responsibility—and one that demands cooperation and reconciliation of competing views and cultures. It goes far beyond simple declarations regarding prohibitions on weapons in space or anti-satellite weapons (ASAT). Space debris poses dangers in space, and when it falls to Earth, it may pose threats to people in its path. Space law and emerging capabilities regarding co-orbital intercept systems, attribution, proportionality, and escalation (res line) all merit significant international attention.

Lastly, no one in the Asia-Pacific Theater can ignore the challenges that weapons of mass destruction (WMD) pose. Cooperative ballistic missile defense (BMD) offers one area of cooperation for peacefully managing the global commons and addressing those who pursue provocative military policies.

Airspace

Closely related to the challenges WMD pose in space, ballistic missiles and cruise missiles could threaten ships at sea, civilian population centers, or military build-up areas.

Fourth generation fighter aircraft and sophisticated air defense weapons could put in question local air supremacy or superiority.

Drones and other remotely operated or unmanned systems provide challenging international issues as we seek terrorists hiding in sanctuaries. We face an immediate future in which domestic airspace will be a focus of the debate about the use of drones. We need to wrestle with the legal and air space management issues associated with these systems operating over the homeland—and the pass-off challenges as the systems cross international boundaries.

Maritime

While state actors have been the traditional threat in regard to interrupting or denying lines of communications and challenging assured access to strategic resources, non-traditional threats are (re-) emerging and worthy of regional efforts to diminish if not deny their effect. Maritime terrorists, modern day pirates, and criminal organizations are appearing with increasing frequency and complicate the defense challenges in the maritime domain. Swarming as an operational tactic has become increasingly relevant. Since the "enemy" often enjoys the advantages of seizing the initiative in battle, our forces must also adopt similar attributes of flexibility and speed (and stealth) to be able to respond in time. This will undoubtedly require cooperation and collaboration in information and intelligence sharing as well as potentially pooling national assets.

Expanded interests in off-shore resource development and exploitation also offer opportunity for cooperation as well as conflict. Be it energy in the Spratly Islands or the Arctic or minerals ripe for deep seabed mining, we will need more cooperation in the future to address the challenges of prosperity, peace, limited resource supply, and growing resource demand.

Land

Perhaps the two most dramatic examples of this changing domain come from Central and South Asia. First, the International Security Assistance Force (ISAF) operation felt the pain of its curtailed land route through Pakistan using Karachi as a port of entry. The Northern Transportation Network, which is much more dependent on air bridges, ultimately proved satisfactory—but at a much higher cost.

Second, as the international community seeks opportunities for the economic development of Afghanistan, it is constantly reminded of the challenges of landlocked states. The future is often linked to a modern day Silk Road, with trucks replacing camels and pack mules as the preferred mode of transportation. Moreover, if Afghanistan can finds ways to unlock its projected mineral wealth, then more will flow on these new roads than silk rugs and tea. Still, the inherent advantages of maritime transportation make forecasting the economic success of a new Silk Road problematic.

CYBER SPACE

U.S. policy spokespersons repeatedly identify cyber as the greatest single security threat. Cyberspace integration brings new levels of vulnerability and the potential for mass disruption of infrastructures or functions across critical military, political and economic targets. Complicating the challenge is that the overwhelming majority of targets are in the private sector, demanding a degree of cooperation and (classified and sensitive) information sharing across boundaries rarely crossed in the past.

The Department of Defense (DOD) Strategy was released in 2011. It is intended for the whole of government and contains five strategic initiatives:

- Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential
- Strategic Initiative 2: Employ new defense operating concepts to protect DOD networks and systems
- Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy
- Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity
- Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation[8]

Strategic Initiative 4 addresses directly the need for international cooperation. As the strategy notes:

"The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence. By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense. Cyberspace is a network of networks that includes thousands of ISPs across the globe; no single state or organization can maintain effective cyber defenses on its own."[9]

At least two specific concerns complicate the problem for international and national security specialists:

- Advanced Persistent Threat (APT)-class malware attacks (targeted, zero-day, stealthy) are real world possibilities
- While cyberspace relies on the digital infrastructure of individual countries, such infrastructure is globally connected

We are faced with similar challenges to those discussed already in the above space section: domain incident characterization; attribution determination; firewalls versus active defense mechanisms in an asymmetric environment; proportionate retaliation; and the enforcement and

[8] Department of Defense Strategy for Operating in Cyberspace, pg. 9.

[9] Ibid.

adjudication mechanisms. Seeking to support responsible behavior and oppose and dissuade those who seek to disrupt network systems, an international cooperation regime would need to share warning capabilities, engage in capacity building, and conduct joint training activities.[10]

Since criminal exploits, military or industrial espionage, critical infrastructure infiltration or sabotage, and nationalist hacker protests might represent elements or techniques of cyber warfare, figuring out appropriate cooperative as opposed to individual responses will be difficult. Such increased sharing and cooperation is far simpler to describe in a strategy document than to implement in practice.

Some of the tough questions that demand common answers follow:

Incident Characterization Cyberspace

- Is cyber warfare characterized as simply "an armed conflict conducted in whole or part by cyber means?" (JCS Joint Terminology)
- In addition to "military operations to deny an opposing force the effective use of cyberspace systems and weapons," how does the world commonly address cyber intrusions on governmental services, financial enterprises, and media outlets?
- Would attacks cross the threshold for an act of war if adversaries cause physical damage to energy, water, or transportation systems?

Attribution Determination Cyberspace

The difficulty in identifying attackers with a high degree of confidence in a timely manner complicates deterrence, preemption, and common response strategies.

- Botnets and proxy servers enable attackers to operate with anonymity and impunity. Advanced persistent threats conceal or avoid detection of attacker identities.
- Challenges in detecting attacks or breaches and attributing correctly delays target identification and retaliatory response.
- Failure to detect intentions, moves and origins stalls preemption and could lead to overreactions and miscalculations.

One solution to the above is resilient, layered, active cyber defenses. Is this a shared responsibility? What is the nature of the (financial) burden sharing?

- Protecting the computers, networks, and control systems in Defense and civilian sectors requires a multi-layered, defense-in-depth strategy that wields active security defenses. What does active defense mean? Sniping?

One place to begin is with protecting civilian and military cyberspace physical assets (computers, servers, controllers, cables, transmitters, satellites and sensors—the potential targets) and their vulnerabilities. Next, national and collective responses are needed to develop capabilities,

[10] See National Security Space Strategy, The White House, January 2011 @ www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

including protocol filters, content sensors, behavioral anomaly scanners, and forensic analysis, to detect and stop, or discover and mitigate, malicious activity. Again, we need a significant investment in resources for these detection capabilities and a common agreement as to what constitutes malicious activity.

Obviously, this demands public, private, and international partnerships that share threat intelligence, analyze vulnerabilities, and identify risk mitigation strategies.

This is far easier to describe in words than execute in practice, particularly in an environment that long operated on a need-to-know basis and very limited sharing across national and bureaucratic boundaries.

Proportionate Retaliation Cyberspace—and the Cross-**Domain Challenge**

Even if the attackers are known with certainty, a challenge exists in determining what incidents justify responses that involve specific uses of force.

- What are the thresholds? Substantial deaths, secondary kinetic damage or cascading economic losses could justify proportionate retaliation by cyber or kinetic means.
- Does a right to counter-strike in self defense exist if attackers target financial systems, public sectors or utilities such as power grids, communications networks, or critical defense industries?
- If origins are traced and force is the response, can collateral damage be avoided or limited to acceptable levels if the intrusions were launched through thousands of hijacked computers in third-country or target nation sites?
- Key role of signaling—how will the various actors in the "partnership" interpret the event and construct a common response that clearly and unambiguously signals intent and intended consequences (in order to avoid an escalation spiral)?

Overlapping Jurisdictions

Transnational cyber incidents underscore overlapping jurisdictions that pose control concerns for prosecution.

- If an attack originates from servers linked to multiple sources, sufficient evidence might not exist to confirm an endorsed attack from a single or multiple sources/governments; and if the source is not a nation, what is the response, and against whom is it targeted?
- Some transnational investigative cooperation is required to enforce a commonly agreed to body of criminal laws and to prosecute actors for attacks generated from sovereign territory, and it is complicated by routing of attack traffic and information acquired through compromised servers in a third-party country. What will be the venue for developing that internationally accepted body of law? How will differing standards of privacy be reconciled?
- Some countries may not be willing to compromise sources and methods to reveal knowledge.
- Some countries may not be willing to acknowledge they are blind to a specific event and need outside assistance (acknowledging a vulnerability).

- The best information may be in hands of private sector (CNN effect); there is a growing body of research about crowd source in the era of social networks that needs common attention[11]
- Prosecution of enraged citizens, dedicated activists, and criminal elements, many of whom reside outside the targeted nation, might not still be feasible given attribution challenges and legal costs. All of this returns to the discussion of failed or near-failed states and their vulnerabilities.

One obvious conclusion to reach is that internationally acceptable rules could promote order in cyberspace by encouraging states to meet their duties in protecting citizens from crime, upholding the right of self-defense, and applying rules of modern warfare. But that will be a long and difficult road to steer.

ROLE OF DEFENSE CAPABILITIES IN CYBERSPACE

Defense capability development considers how to counter competitors who wage warfare in the commons. The identification and fielding of overwhelming force, both as a deterrent and a defensive capability, might include the abilities in the following areas:

- The traditional use of firewalls for data and critical infrastructure protection
- Vulnerability mapping and anomaly detection
- Attack mitigation and resiliency
- Active defenses

It is worth noting that General James Cartwright (USMC, retired), former Vice Chairman of the Joint Chiefs of Staff, noted in May 2012 that the United States needed to protect its military systems, including the stealthy F-35 Joint Strike Fighter, from hackers. "That's the reality of the battlefield we are going to be in." Cartwright went on to add that "in military terms of offense and defense we are thinking 90% defense, 10% offense. That is bass-ackwards for us. Our job is to kill things…."[12] This theme was reinforced with the public release of the Defense Advanced Research Projects Agency's efforts on Plan X. As Ellen Nakashima reports, this is part of an "ambitious effort to develop technologies to improve cyberwarfare capabilities, launch effective attacks and withstand the likely retaliation." Or, as she summarizes, this "push marks a new offensive phase."[13]

One way to move ahead in this new world is to emulate NATO's Smart Defense concept worldwide among partners. According to Henrik Breitenbauch and Bastian Giegerich, Smart Defense is a game-changer regarding defense planning and weapons procurement in that it is based on true international cooperation. They conclude that international burden sharing is a

[11] See for example, "The Rise of Crowdsourcing," @ www.wired.com/wired/archive/14.06/crowds.html.

[12] Walter, Pincus, "Retired General Talks Frankly on Defense," *The Washington Post*, May 22, 2012, P.A13, reporting General Cartwright's remarks to the Joint Warfighting Conference in Norflok, VA, on May 15, 2012.

[13] Ellen Nakashima, "U.S. Builds a Cyber 'Pan X'," *The Washington Post*, May 31, 2012, pp. A1, AA6.

must—and that products and projects must "include partners from two or more allied nations."[14] Some areas for possible collaboration are noted below.

Space Assurance

- Satellite Protection (redundancy, encryption, hardening, and maneuverability)
- Space situational awareness (identifying hazards, determining intent, and attributing actions)
- Operationally responsive (rapid reconstitution capability)

Sea Control

- Operations at greater ranges against advanced maritime recon-strike networks—the 2nd island ring strategy
- Hard-kill fleet protection
- Defeat of combat networks

Air Superiority

- High velocity ballistic and cruise missile interception—kinetic kills
- Enemy air defense degradation or destruction of sophisticated integrated air defense systems
- Evolution and revolution of the Observe, Orient, Decide, Act loop as time compression and the need to shoot first lead us toward rules of engagement and predetermined firing procedures that take humans further from the decision loop to employ lethal force in specific situations
- Penetrating long-range precision attack aircraft that are based outside of immediate kill zones

CONCLUSION

Non-traditional security threats increasingly occupy the time and resources of national security professionals. The cyber domain has the attention of many of us, but other domains also are ripe with threats and opportunities for collaboration and cooperation. Given the broad array of threats across a number of domains the Asia-Pacific region should expand its emphasis in cooperative efforts to reduce the likelihood of war—and if that fails, mitigate its effects. These new threats pose enormous challenges in developing a common value base. Following through with a shared set of responses will require constant vigilance and perhaps nearly instantaneous or even pre-emptive actions in order to protect and advance the security, prosperity, and freedom of like-minded nations and peoples. Ultimately, they may require the supreme sacrifice of blood and treasure. We must hope that we are up to the challenge.

[14] Henrik Breitenbauch and Bastian Giegerich, "A Smart Opportunity," *Defense News*, May 21, 2012, p. 37.