Vision of Future Warfare

Preparing for a Renaissance in Strategic Warfare

Prepared For:

Director, Net Assessment
Office of the Secretary of Defense

Prepared By:

(b) (7)(C)
[redacted]
[redacted]
[redacted]

Date:

July 2012
Revised

Contract No:

HQ0034-ONA-09-BAA-0002

Booz | Allen | Hamilton

Contents

List of Figures

Vision of Future Warfare

I. Introduction and Overview

"The best way to predict the future is to invent it."
--- Theodore Hook

The daunting task before us is to articulate a vision for strategic warfare in the mid-21st century while standing in year 2012. Without Jules Vernes' time machine the team's ability to move forward then back in time to report the facts is a dead end strategy. So how should we proceed?

Our method will be to move down several parallel tracks and from these threads tie a loose bow. First, we will look at the recent past and identify known trends in warfare and technology to ground the reader in a reasonable and defensible view of the present. The nation-state arose out of the post-Westphalian era because in a Darwinian sense it was the most efficient organizational construct for generating political, military, and economic power. Starting in the late 1980's and punctuated on September 11, 2001, non-state actors, while unable to compete with nation-states in their ability to generate military and economic power, have used technology (e.g., information and communications technology) and techniques (e.g., strategic communications) to create a new warfare paradigm that allows them the unprecedented ability to challenge the political status quo of the nation-state. This ability to challenge political power across the global information grid has opened up secondary fronts across the Middle East that are the wellspring from which the Arab Spring[1] has sprung. This ability of disparate interests to coalesce rapidly into a political agenda from whence action can be initiated is a new strategic competition that has, in practical terms, leveled the international political playing field.

Second, to move forward sometimes it is best to look back. It is not that the past is always prologue, but there have been times in the past when new forms of warfare have changed the conflict paradigm. Specifically Giuolo Douhet, William (Billy) Mitchell, and Viscount Hugh Trenchard were able to envision the capability of airpower providing a dramatic break with the past. Trenchard argued in a 1928 Air Doctrine memorandum that, "*Air power can dispense with that intermediate step [ed: defeat of the enemy's army], can pass over the enemy navies and armies and penetrate the air defenses and attack directly the centres of production, transportation and communication from which the enemy war effort is maintained*."[2] Douhet wrote in 1921, "*…If there are nations which can exist untouched by the sea, there are certainly*

[1] *Arab Spring* is the term used in the West to describe a wave of revolutionary demonstrations and protests occurring in the Arab world that began in December 2010. The protests have been mainly forms of civil resistance involving strikes, demonstrations, marches, and rallies, as well as the use of social media to organize, communicate, and raise awareness in the face of state attempts shut down the protests and restrict Internet access.

[2] Chaliand, Gerard. *The Art of War in World History: From Antiquity to the Nuclear Age*. University of California Press, October 7, 1994. Trenchard published little so his views survive mostly through official government memoranda.

none which exist without the breath of air."[3] If one were to substitute the term "air" with the "internet" one can see how the argument could readily apply to our current circumstances. The major revelation that these visionaries were expounding upon was the dramatic break with the past. What was foreseen - the emerging capability of strategic air bombardment - is applicable to the new forms of strategic warfare enabled by cyber and space warfare.[4] The orders of magnitude improvements in economic power that smart technology and ubiquitous information have created presents new avenues for strategic economic warfare that have low barriers to entry and are likely more effective than air power in this role.

This paper posits that a *Renaissance in Strategic Warfare* is underway, and that the United State government must make ready to adapt to the new situation. On the whole, Americans are excellent at adaptation in the face of radical change, so it will not be a difficult thing to do. But understanding the factors in play that are leading to a renaissance in warfare at the strategic level is always helpful. The factors helping to drive and shape this rebirth – the *Renaissance* – include:

- Technical enablement of non-state actors, who are rapidly acquiring the ability to operate at the strategic level, to influence the strategic narrative and to directly impact the actions of nation-states;

- Highly interconnected state and non-state actors on the global stage who simultaneously engage in conflict or cooperation—depending on the issue, circumstance, or convenience—thereby challenging traditional notions of nation-state alliances and coalitions; and

- Recognition that the practice of oversimplifying assumptions and conditions that mask the complex, dynamic interactions at the heart of key issues is counterproductive, and in fact creates more risks than benefits for any player on the world stage.

Ubiquitous communications and social media are driving and will drive fundamental changes in strategic warfare in the future. Progress in robotics and nanotechnology, for instance, may create a credible counter to precision strike weapons, wherein the current paradigm of the *Few, Expensive and Manned* potentially yields to the *Many, Cheaper, and Unmanned* altering the economics and tactics of nation state conflict. At the same time these new capabilities could offer new solutions for contending with networked threats, as opposed to hierarchical organizations, that live in the seams between states and the uncontrolled regions of the world.

In the future, cyber and space warfare permit not just weaker states but also some non-state actors to bypass the military forces of a powerful opponent and to target and damage infrastructure and deny critical services, directly impacting the economy. These changes have a strong undertone of the message presented by Douhet, Mitchell and Trenchard nearly a

[3] Douhet, Guilo. Translated by D. Ferrari. Command of the Air. Coward-McCann, 1942. Douhet's original version in Italian was published in 1921 and not completed translated into English until 1942.

[4] Issues around Space Warfare will not be covered in this report due to the challenges with discussing this topic in an unclassified manner.

century ago; the changes presage a return to the feasibility of homeland-to-homeland strikes (e.g., via cyber attacks); the importance of strategic communications instead of, or as a supplement to, pure kinetic operations; and the growing efficacy and mission scope for semi-autonomous and autonomous capabilities.

Simply stated, it is the intersection of these trends that lead to the renaissance.

We envision a time when the fusion of highly inter-connected, continuously converging computing capabilities with the plethora of new technologies will create a significant shift in the strategic conduct and character of warfare, exemplified by radical changes in the decision dynamics, particularly for nation-states. In this future environment, autonomous machines, rather than man, will be the more significant arbiters of battlefield outcome.

It is hard to discuss the future without some examination of known and likely technology breakthroughs that are likely to occur. Historically, military forces arise out of the skills and capabilities of the economies that spawn them. It has ever been difficult to have and maintain a capability within a military that is absent from how that nation generates and sustains wealth. The use of mercenaries and available technologies can ameliorate this situation to some degree, but this has typically been a stopgap measure. In the end if a society cannot organically create, train, and maintain warfare capability appropriate for the current environment, its military will always be operating from an inferior position.

Beyond the continuing truism of Moore's law,[5] the current trends indicate a continued evolution of unmanned systems operated by remotely located humans into semi-autonomous then autonomous actors on the military stage. This transition will be enabled by significant improvements in energy generation and storage, augmented by innovative information interfaces (both organic and inorganic) as facilitated by nanotechnology processes and holistic 3D manufacturing technologies.

This will be a major watershed in warfare as up until now all warfare has been a human-on-human affair where courage, fear, and the ancient warrior ethos stood as counterpoints to the impact of military technology on conflict outcome. This is the technology track we are on - and as VADM Arthur Cebrowski was wont to say, "*if we are not careful we are going to get to where we are going.*"

Trends in key technological areas such as cyber, space, social media, genomics, nanotechnology, human augmentation and robotics reveal coming changes in how tomorrow's militaries will be equipped and how they will fight, not only because these areas will provide new solutions to military challenges but also because they will change the economies that equip the militaries. These technological trends foretell changes in manufacturing efficiency and effectiveness of current classes of systems that will enable new operational concepts. As these technologies mature new classes of systems move from the merely imaginable to reality.

[5] An observation made by Intel co-founder Gordon Moore in 1965 that steady technological improvements in miniaturization leads to a doubling of the density of transistors on new integrated circuits every 18 months.

We envision a time when the fusion of highly inter-connected, continuously converging computing capabilities with the plethora of new technologies will create a significant shift in the strategic conduct and character of warfare, necessitating radical changes in the decision dynamics, particularly for nation-states. In this future environment, autonomous machines, rather than man, will be the more significant arbiters of battlefield outcome.

One can envision several phases whereby the unmanned systems of today that are surrogates for known capabilities evolve into autonomous, robotic units that give significant leverage to early adopters—and may remove the human element from the immediate battlespace in certain cases. The current U.S.-led paradigm of the *Few, Expensive and Manned* may be eclipsed by a concept of *Many, Cheaper, and Unmanned*.

This is not to say that humans will become irrelevant to warfare, but their role in it will change and that change is likely to have profound political and ethical implications that cannot be ignored.

The major constant in warfare since the first human used a rock has been the element of fear, as all conflict has been a human on human affair. As machines begin to walk the battlefield under their own control this removal of fear changes the character of war at the same time as it threatens the warrior ethos of the military. At the very least, this new environment will require redefining the warrior ethos and culture.

Those who are Junior Officers (JOs) today will be the generals in 2035. Many future U.S. military leaders are gaining critical experiential exposure in Iraq and Afghanistan (e.g., autonomous operations - unmanned aircraft systems) that challenge the warrior culture as well as traditional organizational constructs organized by separate domains (e.g., air, sea, space, land, cyber). This generation of JOs will live the future vision of warfare; they will contend will its challenges and work to take advantage of opportunities in the future security environment. In so doing, they will face a new paradigm in which to develop defense strategy; make acquisition and procurement decisions; engage in planning on force structure, global posture, operational planning; determine their intelligence needs; develop their training and doctrine; and prioritize for future investments via research and development.

II. The World of 2035-2050: Examining the Future Security Environment

"Let our advanced worrying become advanced thinking and planning."

---Winston Churchill

A signature new feature of the future security environment which is unfolding and which will shape the near-to-mid-term is the ability of a wider array of actors, and even individuals, to impact the strategic international environment in ways that limit or force the options of nation-states. A far greater number of actors will have the ability to operate at the strategic level against the United States in the 2035-2050 timeline; technology-enabled adversaries will be in a position to exploit U.S. vulnerabilities (and those of other states)—including attacks on the homeland—in new ways.

The Panoply of Actors

With the 1648 Treaty of Westphalia, the nation-state emerged as the principal organizing construct for the international system and the idea of national sovereignty was born. The end of the 30-Years War ushered in the triumph of the nation-state over global theocracy. Since Westphalia, the nation-state has proved to be the most efficient, effective construct for marshaling political, military, and economic power.

However, experience shows that not every "state" strives to be a nation-state bound by international norms and conventions. The post-Westphalia nation-state has always been challenged by non-state actors, albeit with limited success. For example, while the Balkan nationalists were catalysts of World War I and the shattering of four empires, they had insufficient reach, capabilities, and staying power to dislodge the centrality of the nation-state. More recently, al-Qaida intends to establish an Islamic Caliphate consuming numerous states from North Africa through the Middle East. They are having difficulty in achieving this goal because, among other things, they lack a strategic narrative that resonates widely enough to achieve this vision. The post-World War II process of decolonization, especially in Africa, the Middle East and South Asia, presented a new set of challenges since imperial administrative boundaries did not account for profound tribal, religious, and sometimes ethnic divisions. Nevertheless, a nation-state framework was imposed to facilitate state-to-state relations with the developed world. Due in large part to its ability to withstand challenge, the nation-state system acquired near-global status in the post-World War II period.

However, since the end of the Cold War other entities have emerged on the world stage alongside the nation-state with increased sticking power. The nation-state still remains a predominant feature of the international system – the United States, France, Germany, China, India, Turkey, Brazil, and South Africa provide a few examples. These entities have a history, culture, political structure, and language policies that underscore their unitary (but not necessarily homogenous) nature. They conform to the expectations of international relations and norms.

Today many more categories of state actors exist alongside the nation-state. Two of the most significant to consider in this type of analysis are "*tribal states*" and "*dysfunctional states*." *Tribal states* are entities whose history, including colonization and decolonization, did not produce an organic unitary state but rather one that is composite in nature, with regionalism and tribalism being dominant societal forces. Their official national boundaries often were arbitrarily drawn in the wake of previous wars. These states do not necessarily have a high degree of centralized power and often lack political integration. As a result, their polities can be more susceptible to exploitation or attacks by non-state actors. Examples of *tribal states* include Pakistan, Syria, Iraq, Nigeria, and Libya. "*Dysfunctional states"* are unstable entities, often lacking centralized power, that compete with non-state actors for governance over their territory. Examples of *dysfunctional states* include Afghanistan, Yemen, Somalia, and Mali.

In addition to the types of states described above, non-state actors (both legitimate and nefarious, and increasingly transnational) are becoming a persistent feature of the international system, making the future security environment more complex and less predictable. The potential of non-state actors (e.g., insurgents, terrorist groups, criminals, cartels) is further enhanced by the vast difference in the power, stability, and effectiveness among the different categories of states. Weaker states provide host for non-state actors to ensconce themselves. However, under the current system, the sovereignty of these weaker states must still be respected, creating a barrier to intervention for other nation-states to act. This, combined with the pervasiveness of hyper communication and social media as well as the difficulty modern nation-states face in suppressing these capabilities without undermining the vitality of their own information-based economies, suggests that the newly found potential of non-state actors is likely to persist, if not increase. For example, the Chinese government's massive efforts to control the political content of their citizens' communications provides a real time laboratory for the study of the potential of non-state actors and "netizens"[6] to affect social and even regime change, even as Chinese efforts to erect a "Great Firewall" continue.

Figure 1 below shows the range and breadth of the international actors that nation-states will have to contend with on a regular, and more or less equivalent, basis in the future.

[6] In its simplest form, "netizen" is a combination of (Inter)net and (Cit)izen. Netizen connotes a person that actively participates in the online community of the Internet.

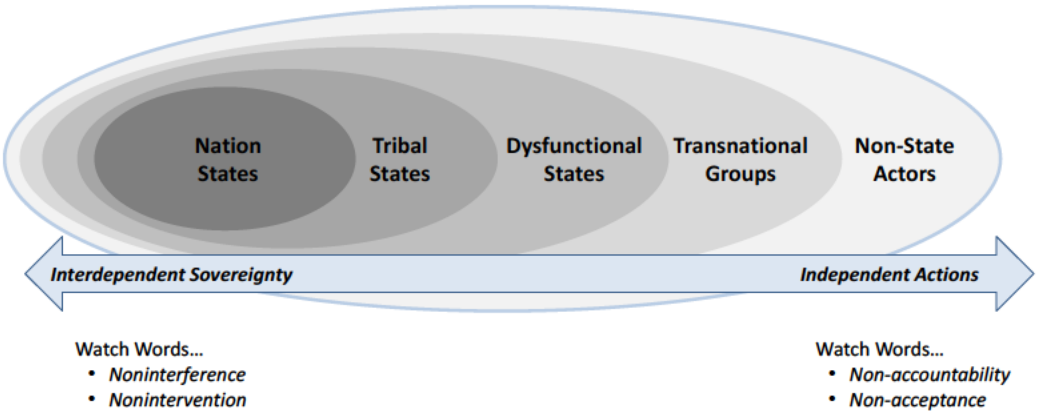


Figure 1: The Continuum of Actors on the Global Stage

(Source: Booz Allen Hamilton)

It is important to note that the panoply of actors described here comprise a continuum. This paper has framed the categories of state and non-state actors for ease and accessibility for the reader. But in reality, there are actors today that fall between various points on the continuum, and this will be the case into the future. For example, "tribalism" can manifest not only in the developing world but in any states that have "tribal" tendencies (e.g. the Basques in Spain, or the Scots of the United Kingdom.) In the past, the United States—and the international community of nations more broadly—have enjoyed the convenience of simply categorizing whether an entity was a nation-state or a non-state actor. The world unfolding before us and projected into the 2035-2050 timeframe is one with greater complexity. Going forward, there will be no easy binning of actors; rather the United States will need to be adaptive in a future security environment characterized by an increasing number of actors on the world stage whose type and shape may evolve along different points on the continuum at different points in time.

III. Critical Future Security Trends and Their Impact

"Always focus on the front windshield and not the review mirror."

— Colin Powell

This chapter identifies trends that will significantly shape the plausible future security environment. The examination is not exhaustive, but rather focuses on major trends that will largely define how the future unfolds. These trends' trajectories provide the backdrop against which to imagine the complexity of the world in 2035-2050, to identify probable sources of future conflict, and to isolate key attributes of future warfare, which, if the United States does not prepare, it will find itself at a distinct disadvantage.

The trends examined in this chapter are: (1) the future of the nation-state; (2) global population growth, urbanization, and the rise of megacities; (3) non-energy resources; (4) energy resources (hydrocarbon energy-focused); and (5) technology (including cyber, space, robotics).

This chapter treats each major trend "bin" independently for clarity and accessibility to the reader. This oversimplification is necessary to help describe how each trend will influence the changing characteristics of conflict from 2035-2050. In reality, each trend is multivariable and, undoubtedly, trends interact. Where feasible, this paper describes those interactions.

The Future of the Nation-State

Adam Smith, in his book Wealth of Nations, points out "*The first duty of a sovereign, that of protecting the society from violence and invasion of other independent societies, can be performed only by means of military forces*."[7] In line with this thinking, a nation-state must maintain a certain level of military strength to meet its obligations as a sovereign. Military strength is a central and essential ingredient of national power.

There are many alternatives by which a nation-state develops its capability to provide for its national defense and ability to project power. However, the composition, shape and size of the military are influenced by two factors, which exist in constant dynamic tension: the perceived need for credible defense and affordability. Generally accepted factors that go into defining the desired level of military capability include a nation's:

- Strategic view of its role and commitments (local, regional or global)
- Threat perception
- Placement on the Geopolitical Continuum
- Socio-political considerations
- Economic status[8]

[7] Smith, Adam. *Wealth of Nations,* edited by C. J. Bullock. Vol. X. The Harvard Classics. New York: P.F. Collier & Son, 1909–14; Bartleby.com, 2001.

[8] "Measuring military expenditure" Stockholm International Peace Research Institute. http://www.sipri.org/research/armaments/milex/researchissues/measuring_milex

While the first four factors work together to define requirements of orders of battle, force levels, and global posture, the fifth factor - economic status – typically emerges as the key limiting factor and often becomes the overriding consideration. In effect, a country's military becomes an expression of its economy.

While the nation-state still has domain over marshaling economic and military power, nation-state preeminence is being challenged—especially in the political and strategic communications realms.

Today, the United States—and the West more broadly—faces the challenge of operating in a world with multiple competing narratives that appear to have veracity.

While the nation-state still has domain over marshaling economic and military power, nation-state preeminence is being challenged—especially in the political and strategic communications realms. The global information and communications revolution is challenging traditional notions of the nation-state and sovereignty. States have not entirely lost their preeminence, as they still define geographic boundaries and maintain military force predominance. Further, nation-states can still develop, articulate, and implement broad strategic direction for their respective countries that can have significant impact on the lives of their citizenry, but increasingly they are in competition with anyone with a political agenda who has access to information technology (Internet, mobile phones, social media). This type of competition can manifest itself in extreme ways, especially in *tribal* and *dysfunctional* states.

Rise of New Political Narratives

The Western world once had a preponderate role in defining the narrative for international affairs. Even during the Cold War, the West used the counter-image of communism as a means of defining its identity and directing the narrative. The United States only had to face a slow-moving, ponderous adversary with a singular narrative, and therefore, only needed to craft a single narrative in response. Today, the United States—and the West more broadly—faces the challenge of operating in a world with multiple competing narratives that appear to have veracity. Besides the quantity, the speed with which narratives emerge and resonate with target audiences is significantly faster.

Over time, more information and media options will challenge traditional notions of national sovereignty, as global information transmissions broadcast national issues (e.g., on human rights, environment, product safety) to international audiences. China's mantra of "non-interference by external parties in its internal affairs" is being eroded not by other nations but by globalized media and communication technologies. Media proliferation and mass communication will enable alternative world views that challenge the predominance of media outlets from the United States and Europe and will provide the means to get the message out to the masses. [9] Arguably, the Muslim world, the dispossessed in Latin America, China, and Russia are leveraging the proliferation of information networks to build competing, authentic narratives that, to a great extent, oppose the U.S./Western view. [10] Governments are ill-suited for the fast pace and dynamic environment of competing narratives; social media such as blogs and tweets, are more critical than official press releases. As a result, the United States has a diminished platform for strategic communications where it can control the narrative.

Governments are ill-suited for the fast pace and dynamic environment of competing narratives; social media such as blogs and tweets, are more critical than official press releases. As a result, the United States has a diminished platform for strategic communications where it can control the narrative.

In addition, more narratives will sustain more dissenting views and support resurgence in local identities, which, in turn, could lead to the emergence of greater numbers of *tribal* and *dysfunctional* states and/or the further empowerment of groups whose political agendas threaten the fabric of the host states in which they reside.

The spontaneous or calculated reaction to a local outrage or to a long-simmering issue is a superb organizing force to mobilize, via hyper communication, large numbers of people against a regime or a specific group -- a process aided by (1) the lack of effective and legitimate sources of central power in certain countries, and (2) explicit prohibition under the Westphalian system for one sovereign nation to interfere with the inner workings of another. The issues in the near term could be a demand for a representative government, a return to a 'golden age' of theocratic rule, or the repression of corruption, which resonate with the population at large and lead to massive public demonstration of their demands. These demonstrations can paralyze societies and produce violent counter-measures on the part of the host state's security forces. Very soon the issues could elevate to those that influence, and in some ways, help define the strategic narrative. The subsequent galvanization of international opinion, immeasurably aided by global communications, constrains the freedom of action of the dominant nation-states forcing, at the very least, their expenditure of resources to support diplomatic efforts to stop the outrages, with increasing risk of direct military involvement in a

[9] Alterman, Jon B. and John W. Garver. "The Vital Triangle: China, The United States and the Middle East." *Center for Strategic and International Studies.* 2008 and Similla-Gonzales, Francis Robert. "Reinscribing Dominant Narratives of the 'Other.'" *Brown University*, April 15, 2011.

[10] Esarey, Ashley. *Testimony before the U.S.-China Economic and Security Review Commission.* Hearing on 'China's Narratives regarding National Security Policy.' U.S.-China Economic and Security Review Commission. March 10, 2011.

campaign over issues of international norms rather than core national interests, which could strain ties with long-standing allies.

The global information and communications revolution has enabled the rise in power of groups and organizations not necessarily aligned with or located within a single national border, in other words, further increasing the panoply of actors. With these technological enablers, transnational groups (legitimate and criminal) as well as individuals can advance their agendas and achieve their objectives on the world stage independently of their host state. These enablers empower transnational groups (e.g., Anonymous and affiliated splinter groups) and terrorists (e.g., Al Qaeda, and affiliated groups). The dissemination of affordable and reliable methods of direct and rapid communication first made possible the popular overthrow of the Marcos government in the Philippines and later bloomed into the color revolutions of Central Asia. Combined with social media more recently, hyper information capabilities provided ad hoc, adaptive, and somewhat resilient infrastructures to resist state-directed violence and to realize regime changes (for example, the Arab Spring), and, in the case of Libya, galvanized the UN and NATO to sanction regime changing military operations.

The communication revolution was supposed to foster a sense of global community, which in some ways it has. But the new communication methods (social media, cyber-enabled communications) have also allowed insular communities with different views of the world to form across borders and regions, some of which are in opposition to the previously dominant United States/Western narrative. The "al Jazeera effect", for example, allowed the Muslim world to use an outside entity (a non-state player) to craft its own narrative for the Iraq war, and international affairs more generally. Information technology and the media revolution have, in fact, enabled these alternative narratives, and led in many places to parochialism rather than an outward orientation. The impact to the nation-state is clear: these developments challenge the ability of the state to speak with one voice and can result in misperception and miscalculation.

Global Population, Urbanization, and the Rise of Megacities

The 21st century is the century of the cities and of urbanization. Five years ago, we saw for the first time more people living in cities than in rural areas. The urban population has expanded in part due to progress in agriculture, the science of nutrition, and medicine—resulting in much higher birthrates. At the same time, the so called "push-factors" (unemployment, low standards of housing and infrastructure, lack of educational facilities) and "pull-factors" (economic opportunities, attractive jobs, better education, and modern lifestyle) are increasing migration from rural

Demographic changes are expected to cause a greater than normal migration to the developed world, both legal and illegal, and, as they migrate, these new residents (as they are not always citizens) will continue impacting the social, political, and economic structures of the societies they join.

areas.

This incredible growth vector places huge burdens on resources of all kinds, and has the ability to redefine competitions over the next couple decades.

According to a recent Rand study, world population growth continues at a significant rate, although it does appear to be slowing somewhat in the aggregate. Recent middle-range estimates indicate that global population could increase from 6 billion now to 7.3 billion in 2025 and 9.4 billion in 2050[11]. Nearly all this growth will take place in the developing world.

The developed world is expecting little or no increase in population (and in some cases a decrease) over the next decade. The population of the developing world, on the other hand, will continue to grow. The recruitment by developed nations of skilled labor from the developing world is expected to continue as the wealthier countries attempt to address the consequences of an aging population. This is expected to cause a greater than normal migration to the developed world, both legal and illegal, and, as they migrate, these new residents (as they are not always citizens) will continue impacting the social, political, and economic structures of the societies they join. States that see a net increase in emigration might experience decreased productivity owing to a shrinking labor pool. States that see a net increase in immigration will probably be concerned about the social and economic impact of an influx of new unskilled workers on their domestic labor markets. Events as diverse as natural disasters or the outbreak of war can spark mass migrations of people to adjacent areas, sometimes across borders and often into areas with little to no capacity to cope with sudden new stresses.

More germane to the future security environment, urbanization continues apace in all types of states (*Nation-states, Tribal states, and Dysfunctional states*), which will impact the future of warfare. The Rand study explains that while urbanization continues throughout the world (see Figure 2 on world urbanization trends), its security implications are probably greatest in developing states. High population growth in agricultural areas, subsequent soil depletion and deforestation, declining agricultural commodity prices, and perceptions that cities offer better economic opportunities have convinced more and more persons in rural areas to migrate to urban ones.

[11] How Demographic Trends Will Change the World Through 2050; http://www.rand.org/publications/randreview/issues/2011/winter/world.html

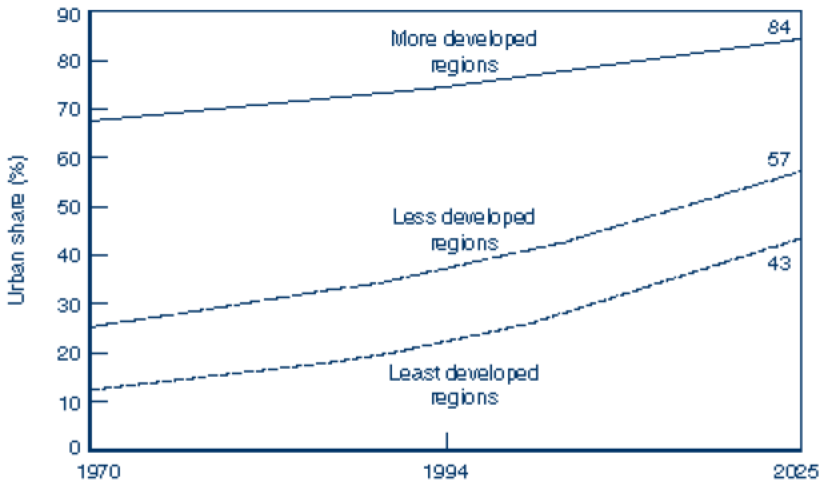


Figure 2: Urbanization Is Proceeding Rapidly in the Developing World

(Source: Rand Study, *Demographics and the Changing National Security Environment*)

According to UN reports, 60% of the global population (approximately 4.9 billion) will live in urban areas by 2030, with the number rising to 70% (or 9.2 billion people) by 2050. Urban areas are expected to absorb all this population growth, and they will continue to attract rural dwellers seeking more lucrative opportunities and better living standards.[12] Population growth will be concentrated in the urban centers of the less developed world, particularly in regions like Asia, Africa, Latin America and the Caribbean.

A corollary to global urbanization is the rise of megacities – urban agglomerations of more than ten million inhabitants. As shown in Figure 3, the UN estimates that by 2015 in the developing world, there will be 23 "megacities" with populations of at least 10 million residents.

The rise of megacities will likely stress the governance capabilities of states, particularly *tribal* and *dysfunctional* states that are already facing powerful centripetal forces.

[12] World Population To 2300, United Nations, Social Affairs, 2004. http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

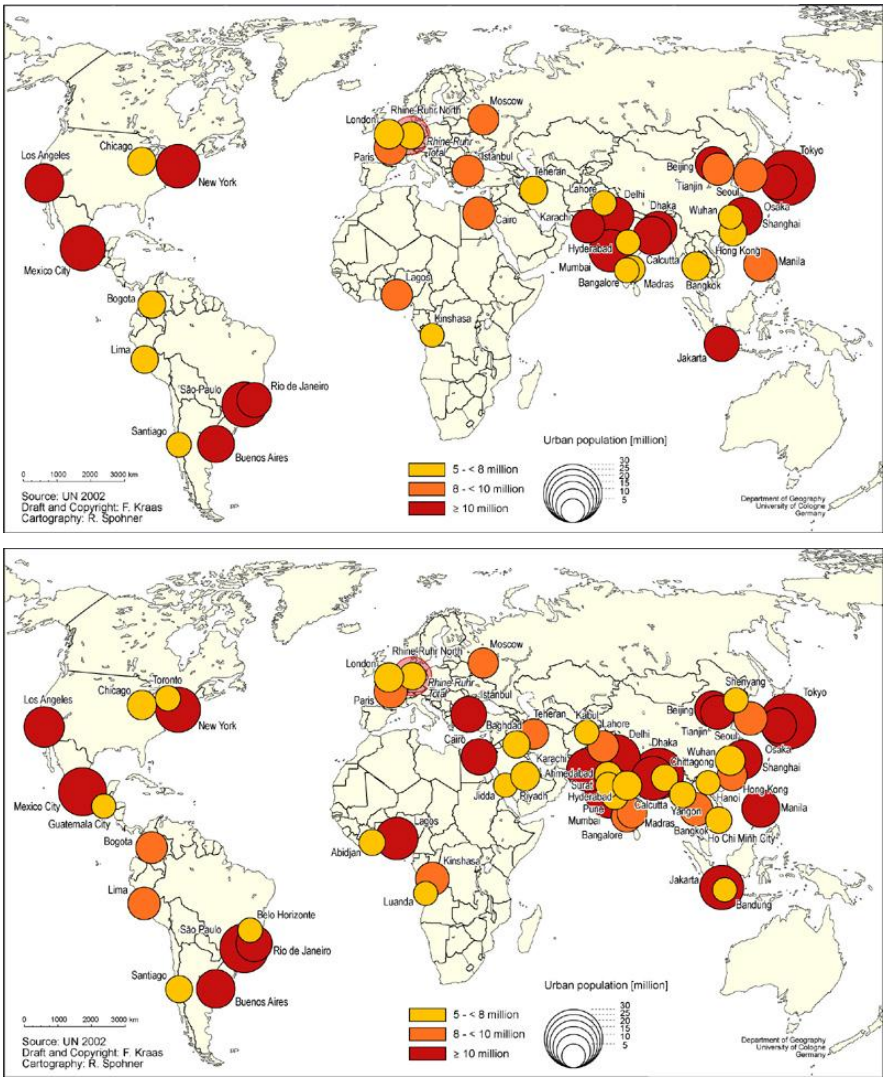


Figure 3: Megacities in 2000 and 2015

(Source: United Nations)

In 2007, there were 19 megacities; the projected number by 2025 is 27. By 2025, 10% of the world's population is expected to reside in megacities. Eighty percent of these projected megacities will be in the developing world. Because these cities are already so large, and because they will be inundated with an overwhelming influx of residents over the next few decades, sizable areas of these cities will be poor, congested, polluted, and poorly served by transportation and housing.[13]

The rise of megacities will likely stress the governance capabilities of states, particularly *tribal* and *dysfunctional* states that are already facing powerful centripetal forces. Megacities can, but not always will, challenge a government's control over these densely populated environs,

[13] The Megacity Task Force, http://www.megacities.uni-koeln.de/index.htm

especially in those states with weak governance. For example, although the Japanese government expertly manages the population of Tokyo, the ability of the Pakistani central government to maintain control over Karachi is questionable at best. As more megacities emerge in the developing world, weak governments will be increasingly challenged to provide services and preserve order. Ultimately, if their central governments fail them, the populations of megacities may turn to local governments or non-state actors grounded in specific (and potentially multiple) identity groups to provide for the common good.

In a highly urbanized world facilitated by the mechanisms made available through globalization, individual actors and non-state actors are able to experience a "jump scale" in effect, exerting influence beyond their previous ability and reach. For example, individual actors are able to exercise influence on a global scale, often through networks that negate the need for geographic proximity. Such a trend has great implications for the future security environment. The degree to which non-state armed groups are able to recruit, procure resources, disseminate ideology, network, and even virtually train members is a case in point. Not only are borders less of an impediment to mobilization, but non-state actors at various scales are increasingly empowered to occupy political space previously reserved for the traditional nation-state. In sum, a new array of actors has the potential to bring mass effects without having to "mass forces" – again demonstrating the shift from *Few, Expensive, and Manned* to *Many, Cheaper, and Unmanned*.

On a more practical front, issues associated with population, urbanization and globalization highlight the question of "upper limits." Basically, how many people can the planet accommodate? While there is no clearly agreed upon limit, some facts do help frame the issue: In 1900, 7.91 hectares of land was available for every person, and by 2005 that share had dropped to 2.02 hectares, and is expected to fall further to 1.63 by 2050. Demand for resources, however, has only been growing, and stands at about 22 hectares per person.[14]

New Sources of Resource Competition

Speaking at last year's World Economic Forum in Davos, President Yudhoyono of Indonesia gave this observation:

> "The world's population is already approaching 7 billion this year, and will go to 9 billion by 2045. Over half are in Asia. Imagine the pressure on food, energy, water and resources. The next economic war or conflict can be over the race for scarce resources, if we don't manage it together."[15]

[14] UNEP (2007) Global Environment Outlook: environment for development (GEO-4). UNEP. http://www.unep.org/geo/geo4/media/

[15] President Yudhoyono of Indonesia speaking at the World Economic Forum in Davos, 28th January 2011.

Countries which have exhausted their own resources, or whose domestic stocks are not sufficient to meet the domestic demand without imports to complement them, could seek materials, food and energy beyond their own borders, and this effort to acquire these additional resources could either be accomplished peacefully or through military conquest intimidation. This has been a common practice since the days of the Roman Empire, and colonialism's "scramble for Africa." A very clear implication of all this is that the competition for resources will become an increasingly important factor in international relations, and the future security environment.

The nexus between critical resources and unsettled territorial disputes (ever more frequently involving complex Law of the Sea issues) presents a primary source of potential future conflict. At issue is the ownership of, and therefore assured cheap access to, carbon based energy sources (still primarily oil and gas in terms of potential for conflict), critical minerals (not only 'rare' minerals but also more mundane material like copper, iron, and titanium) agricultural and potable water supply.

The nexus between critical resources and unsettled territorial disputes (ever more frequently involving complex Law of the Sea issues) presents a primary source of potential future conflict.

Geographic areas of current and potential resource competition include the Arctic, the Antarctic, the South Atlantic, and the South China Sea, with the vast reaches of the Pacific presenting future challenges of ownership of resources distant from interested states. Land-based intersections of potential resource-based conflict include the Jordan River, the Mekong, and, potentially, the rivers of Central Asia.

Beijing has significant concern for and desire to secure Chinese sea lines of communication. Distrusting the United States' guarantee to safeguard freedom of the sea to one and all, the Chinese seek to increase their capability to protect their global interests. The rise of a new global power is inherently destabilizing as the power balance is recalibrated, increasing, at least temporarily, the risks of miscalculation in a crisis or from confrontations stemming from Beijing's imperial overreach.

Non-Energy Resources

Demand for non-energy resources has skyrocketed over the last decade. World mine production of iron ore, for example, has increased by nearly 160 percent since 2001, while prices have increased 263 percent over the same period.[16] China's ongoing industrialization—coupled with the depletion of many of its domestic reserves—accounts for much of this demand growth. China has responded to its increasing dependence on imported resources in various ways, including signing long-term supply agreements with foreign producers, acquiring foreign mining assets, and actively exploring for new resources at home and abroad.

[16] Mine 2011 The game has changed: Review of global trends in the mining industry, PriceWaterhouseCoopers, http://www.pwc.com/en_GX/gx/mining/pdf/mine-2011-game-has-changed.pdf

International producers (e.g., Australia, South Africa), meanwhile, have been opening their doors wider than ever to take advantage of the opportunities China's growth presents.

Critical Minerals

History is replete with examples of minerals playing a critical role in international competition over scarce resources, and also setting the international political agenda. Minerals are part of virtually every product we use. Their unique properties contribute to provision of food, shelter, infrastructure, transportation, communications, health care, and defense. Minerals used in common applications include iron to produce steel, copper used in electrical wiring and plumbing, and titanium used for the structural frames of airplanes and in paint pigments. Every year over 25,000 pounds (11.3 metric tons) of new minerals must be provided for every person in the United States to make the items that we use every day, and a growing number of these minerals are imported.[17]

Minerals and useful materials derived from them – mineral commodities – are the physical and economic foundations of society. For example, the U. S. Geological Survey (USGS) compiles production and consumption data for 84 mineral commodities used in America (Mineral Commodity Summaries). These include metals like iron and copper but also many less well known elements such as indium and scandium. Some of these mineral commodities are not only important to our everyday life (e.g., it takes about 60 elements obtained from minerals to make a cell phone) but they also face potential supply restrictions. These are called "critical mineral commodities" or just "critical minerals."

The economic importance of critical minerals, increasing global competition for them by rapidly developing countries, and the potential for supply disruptions triggered a recent study by the National Research Council (NRC). The final report of this study – *Minerals, Critical Minerals, and the U.S. Economy* – developed a method for characterizing a mineral's "criticality". The method evaluates a mineral's importance and its availability at a specific scale (such as nationally) and time (such as the near term from one to several years).

A mineral commodity's importance can be characterized by factors such as the dollar value of its U.S. consumption, the ease with which other minerals can be substituted for it, and the outlook for emerging uses that can increase its demand. A way to evaluate the significance of these factors is to consider the impact that a lack of availability would have on them. How would the mineral's uses or price change if it were less available?

A mineral's availability depends on several factors including how much has been discovered, how efficiently it can be produced, how environmentally and socially acceptable its production is, and how governments influence its production and trade. Many of the technological, social, and political factors have become increasingly important influences on mineral availability. For example, China produces most of the world's rare earth elements (the United States imports 92% of its rare earths from China). By curtailing export shipments of these technologically key elements in 2010, China drastically affected their global availability.

[17] Ibid

The criticality evaluation method developed by the NRC study relates the importance and availability of a mineral in a "criticality matrix" (Figure 4). The matrix uses evaluations of the impacts of supply restrictions (the importance of the mineral) to the potential for supply disruptions. The greater both of these measures are the more critical the mineral is. The criticality assessments included in Figure 4 are for selected mineral commodities and show that platinum-group and rare earth elements are much more critical mineral commodities than others such as copper, titanium, and lithium.

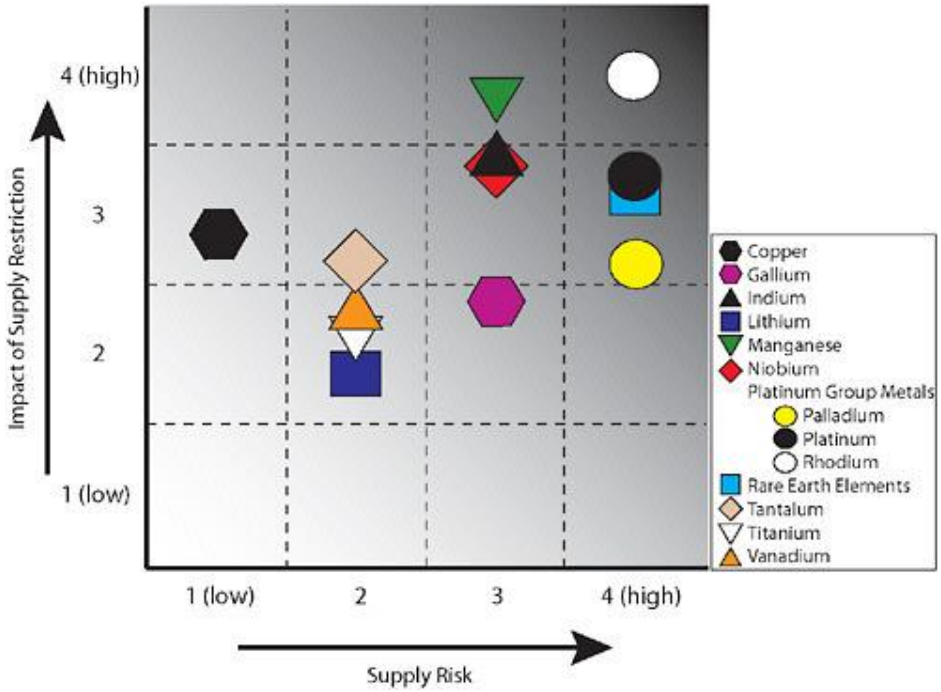


Figure 4: Criticality Matrix for Eleven Mineral Commodities

(Source: National Research Council Report: Minerals, Critical Minerals, and the U. S. Economy, 2008)

The global nature of the nonfuel minerals market has been made very evident in recent years, as many emerging economies have become both significant producers and consumers of various raw mineral products, in some cases competing for mineral feedstock directly with U.S. producers, manufacturers, and users. While foreign competition for minerals is one aspect to consider in the range of factors affecting supply of minerals to the U.S. economy, a high degree of import dependence for certain minerals is not, in itself, a cause for concern. However, import dependence can expose a range of U.S. industries to political, economic and other risks that vary according to the particular situation. The bottom line is that if the supply of any "critical minerals" used in strategically important products and services was curtailed, the military, consumers and various sectors of the U.S. economy could be significantly affected.

Recent tensions with China concerning the supply of rare earth elements serve to highlight the true nature of the issue. As evidenced by a recent National Academy study, the United States' import dependence is neither inherently problematic nor are rare earth minerals geologically

scarce. Rather, the real issue is that U.S. supply options for rare earths are limited: supplies are concentrated mostly in the hands of one supplier with its own rising demand, and the United States currently has no good options for recycling rare earth minerals or substituting more easily obtained minerals. While China is nearly the sole producer and exporter of rare earths today, it does not possess a permanent "corner" on this market. Indeed, China holds only about half of known world reserves. The loss of China as a supplier might increase the costs of rare earth minerals, but would not necessarily impact their near-term availability. The issue, then, is more appropriately understood in terms of managing risks such as depletion and wide scale disruptions and ensuring that the U.S. government's most important defense and energy needs can be met.

In worst-case scenarios, supplies of minerals that the United States does not produce domestically may be disrupted, creating price spikes and lags in delivery. Even short of major supply disruptions, supplier countries can exert leverage over the United States by threatening to cut off certain key mineral supplies. The United States may also lose ground strategically if it continues to lag in managing mineral issues, as countries that consider assured access to minerals far more strategically important than the United States does are increasingly setting the rules for trade in this area. China's rising dominance is at the heart of this growing public debate.

Water

Water is a critical shared resource due to its role in basic survival, but it is different than other non-energy resources in that it is generally not traded; moreover, states that share water often have considerably different priorities and interests. For many years international war over water has been touted as the next impending "crisis" facing the world, but the reality appears more ambiguous. The warnings have consistently fallen short; in fact, more cooperation than warfare has occurred. In recent history, there are no examples of two states going to war specifically over water resources. Instead of resorting to war, historically states have developed ways to manage water scarcity or have decided to cooperate. At most, water issues have exacerbated existing tensions and sometimes can be considered a contributing factor. Violence over water does occur; however, it is almost always internal to states—for example, competition between farmers and industrialized areas, leading to localized disturbances.

Before dismissing the concerns over conflicts related to water, it is important to take into account the growth in population. The reality is that the world will likely have a population of 7.3 billion people by 2025 and 9.4 billion by 2050, with nearly all this growth taking place in the developing world. As a result, it is very likely that nations will face water scarcity issues and the stress associated with that challenge. Assuming that because war over water has not occurred it will never occur seems premature due to the scale and complexity of the issue.[18] Moreover, there are numerous examples of intrastate violence caused by water scarcity. Cooperation on water issues has remained incomplete; national interests still often hold sway. Consequently, one could envision a scenario in which an interstate conflict arising from water scarcity leads to domestic unrest that threatens regime survival.

Cooperation on water issues has remained incomplete; national interests still often hold sway. Consequently, one could envision a scenario in which an interstate conflict arising from water scarcity leads to domestic unrest that threatens regime survival.

While the greatest tensions with regard to water lie in the Middle East or Africa, Asia faces significant water scarcity issues because two-thirds of the world's population underserved by water lives in this region. The majority of water resource issues in Asia are intra-state rather than inter-state. However, the two examples below illustrate the potential for, and difficulties with, increased cooperation over water and the potential for tensions and conflict.

- The Mekong river basin provides critical economic and agricultural support and, foremost, basic survival to some 250 million people in Cambodia, China (the Yunnan Province), Laos, Burma, Thailand, and Vietnam.[19] Although these states have geopolitical tensions to varying degrees, none have threatened to go to war over water. In fact, these states have attempted to integrate their river and water use management by establishing the Mekong River Commission (MRC) in 1995 (its predecessor dates to 1957), composed of Cambodia, Laos, Thailand, and Vietnam; China and Burma are Dialogue Partners. The MRC has functioned as the focus of research, developmental programs, and high-level political dialogue regarding the Mekong. Nevertheless, it still has fallen short of being able to forge a unified policy that all parties consider equitable. Like many international organizations, the MRC is only as effective as the member states' will and capacity to work collaboratively and place regional interests over national interests when needed. For example, China has plans to build 14 dams on the upper Mekong that will have cascading ecological and economic effects on the downstream states, but Beijing has done little to coordinate its dam construction formally with the other states.

- Management of the Ganges River, which supports several hundred million people in both India and Bangladesh, approximately eight percent of the world's population, has

[18] Rai, Neena. "Water Wars May Lie Ahead." *Wall Street Journal,* June 29, 2011.

[19] Cronin, Richard and Timothy Hamlin. "Mekong Tipping Point." Stimson Center, 2010.

been a long-running dispute between the two states.[20] Bangladesh, the downstream and much weaker state, desperately needs the Ganges' water, and its problems are exacerbated by the fact that it is one of most densely populated states and its water tables are dropping. India, being upstream and stronger, can leave Bangladesh at its mercy as New Delhi uses the water to support the millions of people who rely on the Ganges for their survival and livelihood (primarily agricultural).[21] Since 1960, India and Bangladesh (part of Pakistan until 1971) have negotiated over a management program. An agreement was reached in 1977, lapsed in 1988, and then a 30-year agreement was reached in 1996. Nevertheless, the situation has not been permanently resolved, and tensions remain. For example, India is planning on a major canal building project to link several rivers, including the Ganges, to mitigate the impact of droughts, and Bangladesh fears this will affect the downstream flow of water.[22] The poverty-stricken Bangladesh will almost certainly not initiate a war with India, but water scarcity can lead to much stress and instability in Bangladesh. For example, mass migrations in Bangladesh caused by a lack of water could easily exacerbate the existing and deep ethnic tensions between the two states, especially if Bangladeshis attempt to flee their country.

Energy Resources (Carbon-Based Energy)

No so single resource embodies the nature of the international resource competition better than energy resources. Given global energy infrastructures and the preponderance of fossil fuel-based economies, carbon-based energy competition has been, and will continue to be, a major element of the future security environment. Trends in this area have been well studied, and are generally known. This paper touches on some key aspects of the overall trends, without attempting to repeat what is fairly well understood by most security analysts.

Overall Energy Trends

Given the tremendous impact carbon-based energy resources have on the dynamics of international relations, exploring what is likely to occur with regard to this precious commodity is essential to understanding conflict in the future. According to BP's report on the future trends in energy (BP Energy Outlook 2030, London, January 2012) there are some key points to keep in mind about energy consumption over the next 20 years.[23]

First and foremost, who is using the energy? *The economies of states not belonging to the Organisation of Economic Co-Operation and Development (OECD) drive energy consumption growth as the fuel mix gradually shifts away from oil and coal.* Some key points on this shift include:

---

[20] Akanda, Ali Shafqat, and Justine Treadwell. "Contributing Factors in the Ongoing Water Conflict Between Bangladesh and India." Tuffs University, March 2009.

[21] Ofori-Amoah, Abigail, "Water Wars and International Conflicts." University of Wisconsin, Eau Claire, USA, Spring 2004.

[22] Mandhana, Niharika. "Water Wars: Why India and Pakistan Are Squaring Off Over Their Rivers." *Time,* April 16, 2012.

[23] http://www.bp.com/liveassets/bp_internet/globalbp/STAGING/global_assets/downloads/O/012_2030_energy_outlook_booklet.pdf

- World primary energy consumption is projected to grow by 1.6% per annum (p.a.) over the period 2010 to 2030, adding 39% to global consumption by 2030. The rate of growth declines, from 2.5% p.a. over the past decade, to 2.0% p.a. over the next decade, and 1.3% p.a. from 2020 to 2030.
- Almost all (96%) of the growth is in non-OECD countries. By 2030 non-OECD energy consumption will be 69% above the 2010 level, with growth averaging 2.7% p.a. (or 1.6% p.a. per capita), and will account for 65% of world consumption (compared to 54% in 2010).
- OECD member countries' energy consumption in 2030 will be just 4% higher than in 2010, with growth averaging 0.2% p.a. to 2030. OECD energy consumption per capita will be on a declining trend (-0.2% p.a. 2010-30).
- Gas and non-fossil fuels will gain share at the expense of coal and oil. The fastest growing fuels are renewables (including biofuels) which are expected to grow at 8.2% p.a. 2010-30; among fossil fuels, gas will grow the fastest (2.1% p.a.), oil the slowest (0.7% p.a.).

To appreciate fully the impact of the consumption, it is essential to see what the energy is being used for. *The growth of energy consumption by sector is dominated by power generation and industry.*

- Energy used to generate electricity remains the fastest growing sector, accounting for 57% of the projected growth in primary energy consumption to 2030 (compared to 54% for 1990-2010).
- The power sector is also the main driver of diversification of the fuel mix; non-fossil fuels, led by renewables, account for more than half of the growth. Industry leads the growth of final energy consumption, particularly in rapidly developing economies.
- The industrial sector will account for 60% of the projected growth of final energy demand to 2030. The transport sector shows the weakest growth, with OECD transport sector demand projected to decline.
- Diversification is beginning in transport, driven by policy and enabled by technology: biofuels account for 23% of transport energy demand growth (with gas contributing 13% and electricity 2%).

In short, consumption is being driven largely by non-producing countries, and the use of the fuel is primarily aimed at driving the economic growth strategies of these countries. This combination creates some worrisome incentives for behavior, based on how 'at-risk' the counties consider their supply chains to be.

Oil Access and Ownership

Two decades from now there may be as much annual supply of crude oil as there is this year, but the landscape of access and ownership will be radically different. A ready supply of crude oil is based on the existence of known reserves, the technology to extract it, and the market forces that make the extraction a profitable investment. Huge reserves of oil have been found off the coast of Brazil, in the Gulf of Mexico, and in the seas of western Africa. Moreover, recent, almost dramatic, advances in the technology necessary to extract that oil thousands of

feet below the surface has only recently come into operation, enabling Brazil, for example, to begin recovering and sending to market the deep-sea oil only recently discovered off its coast. In the timeframe being examined in this report, it is quite likely that the technology for such deep water extraction will only spread, become less expensive, and be surpassed by new technological extraction methods as well.

The more relevant future concern about oil, at least in terms of trending, should not be how much there is but who will control it at various stages of the supply chain – from the drilling field, to the tankers and pipelines that transport it, to the refineries that transform the crude into commercially usable fuels.

As a result, the more relevant future concern about oil, at least in terms of trending, should not be how much there is but who will control it at various stages of the supply chain – from the drilling field, to the tankers and pipelines that transport it, to the refineries that transform the crude into commercially usable fuels. The fight for oil "ownership" has picked up recently.

If current trends continue, the Chinese may well have doubled or tripled their demand on the world's crude oil market. The primary obstacle to that happening is that Western oil firms such as Exxon Mobil and BP will get into bidding wars with China-based oil operations for new deposits but that bidding could become extraordinarily expensive.

For example, in late 2009, Exxon agreed to buy a one-quarter stake in the Jubilee field (which is estimated to hold more than 1.2 billion barrels of oil) in the ocean off Ghana for $4 billion. Sinopec, a leading Chinese oil company and BP came in later bidding for the same ownership. Exxon-Mobil abandoned its offer in August 2010, opening the way for a Ghana National Petroleum Corporation (GNPC) bid backed by the China National Offshore Oil Corporation (CNOOC). CNOOC would take a 10% stake, another major oil company 10% and GNPC 3% of Jubilee.[24]

China's oil interests are busy in every region of the world where large new crude deposits are in the early stages of exploration and recovery. In early 2012, the China Development Bank made a $10 billion loan to Brazilian oil company Petrobras to help it produce crude from its recently discovered deep-sea deposits.[25] Sinopec will buy 150,000 barrels a day from Petrobras in the first year of their partnership and 200,000 barrels a day in the nine years after that as part of the deal. The precursor to the deal goes back to 2009, when China helped Petrobras address tight credit markets to finance a $224 billion investment plan.[26]

---

[24] http://www.thenewcrusadingguideonline.com/index.php?option=com_content&view=article&id=207:in-the-name-of-oil-ghana-is-already-swimming-in-a-flood-of-debt&catid=70:business-a-money&Itemid=73

[25] Bloomberg, China, Brazil Agree to $10 Billion Loan, Exploration, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a1BzJNEdbjsc

[26] Ibid

China's actions in the global energy market point to an attempt to influence increasingly this market (particularly for oil) in its favor as part of its overall energy security policy. Given both the critical role of oil to the growing Chinese economy, Beijing has been forced increasingly to turn to the Middle East and Africa for supplies. However, its critical dependence on others to provide the commodity creates a strategic risk for China – a risk that Beijing likely feels must be addressed by owning its own supplies. China has substantial domestic stocks of oil and coal yet these stocks cannot keep pace with its growing economy, hence China's need to rely increasingly on imported energy to make up the difference. The Middle East is anticipated to be the major source of imported oil for China for the foreseeable future, and China is attempting to mitigate the risks associated with being so dependent on such an unstable part of the world by trying to develop additional sources of oil, particularly in Africa. However, it should be anticipated that China will play an increasingly role in Middle East affairs, which raises the possibility that China could be dragged into a conflict in that region.

Moreover, many energy analysts in China believe that the South China Sea could contain the equivalent to Saudi Arabia's worth of oil beneath the sea floor. Given that China and other Southeast Asian nations are in dispute about the status of maritime boundaries in that Sea, the prospect of tensions over those disputed boundaries, coupled with the increased extraction of oil and/or gas, could also embroil China or other major powers in a conflict over dominance in the South China Sea/Southeast Asia region.

A Navigable Arctic

Commercial ships could be sailing across an ice-free Artic as soon as 2035, according to United States Navy estimates, transforming the shipping rates and routes between Europe and the Far East.[27] The prediction, made by the head of the Navy's climate change task force, highlights the growing international interest in the commercial opportunities created by shrinking Arctic sea ice.

The Arctic sea ice extent observed by satellites has been shrinking for the past 30 years, with coverage at its lowest in the satellite record. This reduction is occurring at least 30 years earlier than was anticipated in the recent assessment report issued by the Intergovernmental Panel on Climate Change. These sea ice minima open more than 40% of the Arctic Ocean to increased absorption of warmth from the sun near the end of summer. Extensive open water has been observed in the Chukchi Sea, the East Siberian Sea and north of the Barents Sea.

As the summer melt season lengthens and intensifies, there is less sea ice at summer's end. Major delays have occurred in the timing of fall freeze-up since 2005. Over 40% of the thick sea ice that was built up over many winters (nearly 10 feet thick), has melted and is replaced with thinner ice formed in a single year.

[27] http://www.ft.com/cms/s/0/730ef8fe-27e1-11e0-8abc-00144feab49a.html#ixzz1rNZh5rDn

The National Oceanic and Atmospheric Administration (NOAA) reports that, using the observed 2007/2008 summer sea ice extents as a starting point, computer models predict that the Arctic could be nearly sea ice free in summertime within 30 years (See figure 5 below). [28]

These same computer simulations indicate that Arctic sea ice retreat will not continue at a constant rate into the future. Instead they show several abrupt decreases in summer Arctic sea ice cover in the future. The projections for a likely ice retreat suggest that the Arctic could transition from perennial year-round ice to seasonal winter ice, with numerous implications for the climate system.

Sea ice minima in September of 1980, 2007 and 2008. Sea ice images from NASA/ Goddard Space Flight Center Scientific Visualization Studio

Model projections of sea ice thickness when the Arctic is nearly ice free in September, within 30 years. Units for sea ice thickness are meters.

Figure 5: Arctic Ice Mass Past, Recent and Projected

(Source: http://www.arctic.noaa.gov/future/sea_ice.html)

As sea ice melts in the Arctic, a new economy is emerging. The nations bordering the Arctic are drilling for oil and gas, and mining, shipping, and cruising in the region. Russia, Canada, and Norway are growing their icebreaker fleets and shore-based infrastructure to support these enterprises. For the United States, the economic potential from the energy and mineral resources is in the trillions of dollars. The U.S. Geological Survey estimates that nearly 30 percent of the world's undiscovered natural gas and 13 percent of the world's undiscovered oil resources are in the Arctic.[29] In addition, the Arctic holds rare earth minerals, and massive renewable wind, tidal, and geothermal energy.

The United Nations Convention on the Law of the Sea (UNCLOS) provides the framework for global governance of the Arctic. This agreement updated and expanded a series of conventions that had been created in 1958. In addition, UNCLOS established a consistent set of limits for territorial and contiguous seas, navigation rights, seabed usage, and dispute adjudication. Arctic states have accepted UNCLOS as a suitable regime for managing the region. UNCLOS

[28] http://www.arctic.noaa.gov/future/sea_ice.html

[29] *U.S. Geological Survey*. "90 Billion Barrels of Oil and 1,670 Trillion Cubic Feet of Natural Gas Assessed in the Artic." USGS Newsroom, July 23, 2008.

gives authority to littoral states for most governance issues, but does not lay out details on how the Arctic should be managed or controlled.

Perhaps the most significant portion of the UNCLOS agreement is the creation of a set of definable limits for maritime boundaries. Article 3 of the agreement limits the breadth of the territorial sea to 12 nautical miles. To compensate for this relatively short expanse, Part V of the Convention established the exclusive economic zone (EEZ), an area beyond the territorial sea with a breadth of 200 nautical miles. States have sole rights over the exploitation of all the resources in their EEZ, whether natural or mineral.

The majority of the resources in the Arctic are located clearly within the bounds of territorial seas or exclusive economic zones (EEZ).

Russia is currently the most assertive and aggressive player in the Arctic; they also have the largest and most effective fleet of ice-breakers in the world. Controlling the Arctic is a geostrategic priority and a matter of national prestige for Moscow. The Arctic is also critically important to Russia's future economic success. Canada has shown a willingness to act unilaterally in the Arctic, perceiving the United States as its most significant regional competitor, although it also seeks to engage with Washington on Arctic issues. Ottawa's outlook on the region, which is central to its national identity, is complicated by the lack of capacity to control its interests in the Arctic unilaterally.

Strategic interests may trump economic viability in determining whether a nation will exploit or develop the Arctic's natural reserves. Concerns over national prestige and identity may also cause countries to take actions that may not appear to be in their best strategic or economic interests.

Critical Operating Domains

Throughout history, the chief source of geopolitical advantage for dominant empires and nation-states has been their ability to seize the advantages of new technologies, operational innovations, and organizational models to expand—and ultimately transform—their social, economic, military, and diplomatic capabilities. The domestication of the horse, use of chariots, and new economic models of agro-pastoralism changed society and warfare in the Bronze Age and gave greater significance to armies and "land power" in the Middle Ages. New seafaring technologies and techniques, and economic models of mercantilism and commerce, shifted the geopolitical balance to the maritime world by the sixteenth century, demonstrating the significance of "sea power." Likewise, the invention of the internal combustion engine and the development of the automotive and aerospace industries transformed the economy, society, and national security in the twentieth century, giving rise to the notions of "air" power.

In each of these eras, clearly defined "domains" emerged land, sea, and air. Influence and power shifted to those nations that successfully developed economic concepts, diplomatic rules, military doctrine, and international and national institutions for exploiting new technologies and processes within those domains. Following this historical course, two new domains have emerged out of the latest technological revolution: the cyber and space domains.

Cyber and space are global capabilities and global enablers that together enable the U.S. military to maintain a strategic advantage over potential adversaries and improve U.S. national security. Technologies associated with these capabilities truly define the leading edge. Cyber and space capabilities are also central to the U.S. military operating environment. Information regarding an adversary's activities can be sent from a computer in Tampa, and may be directed through a local network, transmitted by satellite, and then received by a Commander in the field halfway around the world.

Space capabilities supplement and enhance cyber capabilities, and vice versa. The timing function provided by GPS enables all of the base stations in a data network to stay synchronized. This is done largely through the shared electromagnetic spectrum and IT infrastructure, which creates a wide range of cross-domain vulnerabilities. An attack on U.S. space capabilities may start in cyber domain, and attempts to hack U.S. cyber capabilities get routed through the space domain.

Access to these critical domains is quite easily acquired for both states and non-state actors to contest our use of both space and cyberspace. The low barriers to entry for cyber capabilities are well known and documented. The impact of affordable and scalable technology means all adversaries have effective capabilities against networks and computer systems. The conventional wisdom surrounding space capabilities is that only highly developed industrial countries can have a stake in the space domain (i.e., to put satellites in orbit and maintain them). On its face, this makes sense. However counter-space capabilities do not always require having a space program. The space domain's connection with cyber combined with its terrestrial components means there is a potentially low barrier to entry for disrupting activities in the space domain using equipment that state and non-state actors can easily acquire.

Cyber

If the world is currently experiencing what some call the *Information Age*, the future will no doubt be seen as the *Connected Age*. In this setting, operating environments become hyper-connected networks. As a result, the convergence of people, hardware, information, software, and insight will likely drive the future global economy. Throughout the world businesses, organizations, and governments have expanded and altered their operating models to take advantage of the so-called 'network-effect.' These network-enabled changes have dramatically improved efficiency and effectiveness and enabled wide spread innovation, spurring the creation and expansion of whole industries. New opportunities arise daily from the ability to collaborate at a speed, scope, and scale never previously seen.

Globalization is a process of increased connectivity and interdependence transcending social, economic, and political spheres. While globalization is not a new phenomenon, the current wave of globalization has achieved an unprecedented speed and scope of effect. Rapid advances in telecommunication and transportation technologies have compressed traditional perceptions of time and space, allowing interactions to occur virtually, in real time, and across cultural barriers.

This has had a profound impact on day-to-day economic transactions and has greatly accelerated the integration of global markets. An erosion of conventional political boundaries

has further facilitated the flow of goods, services, capital, people and – most importantly – ideas. While such an integrated system has clear benefits, it also brings into focus the degree of material and political disparity that exists both domestically and globally. Furthermore, the benefit accrued by this integrated environment is somewhat offset by a diminished capacity to keep potential threats at a distance due to the high degree of connectivity. To be competitive in the face of great disparity in international wage structures, the leading economies, especially the United States, have become dependent on complex global links supporting 'on demand supply' (to reduce inventory costs) and robotization (to reduce labor costs). Superbly efficient in peace, this interdependent economic system has significant potential vulnerabilities in crises and in war that could be exploited by rival states and even by some non-state actors.

The combination of rapid, assured global communication, coupled with the ever enhancing capabilities of cyber warfare makes possible highly effective, rapid, and continuous strategic strikes against an enemy's political, military, financial, economic, and social centers of gravity.

The combination of rapid, assured global communication, coupled with the ever enhancing capabilities of cyber warfare makes possible highly effective, rapid, and continuous strategic strikes against an enemy's political, military, financial, economic, and social centers of gravity. For example, in the economic realm, the interface of the global information grid with the physical control system, global supply chains, and single-link production and distribution systems offer extraordinarily rich targets for cyber warfare via electronic strikes from abroad, pre-planted destructive programs, targeted special operations to cause substantial physical damage to key infrastructure, 5th column electronic saboteurs, or —for those states with the capability—anti-space activity (e.g. attacks on the downlinks from space). Properly focused attacks on a nation's electric distribution grid could cripple the system and result in a rapid shutdown of its economy; restoration of that capability could prove to be a long, difficult task. Thus, the "home front" becomes a front line on day one of a conflict, and not from attacks by manned platforms (e.g. B-17s coming in from overhead). Warfare against nation-states, particularly among major powers, is going to have these dimensions to it – probably sooner than 2035.

The increase in cyber-enabled integration also increases "insider threats" (e.g., sleeper cells in the United States or intrusions into U.S. systems – government or private sector – via cyber. As the United States moves toward greater cloud computing and cloud services, it is expanding U.S. borders to include others; the idea of a "fortress mentality" disappears. If the United States were to opt to fortress or enclave itself, it would forfeit its ability to leverage the very technology that promises to underpin its economic vitality.

Space

The promise of modernity, progress, and near-limitless possibilities offered by the Soviet Sputnik and the American Mercury programs at the dawning of the space age have been more than realized in the unfolding of the post-Industrial Age. The world's governments, militaries,

economies, and societies themselves have grown ever more reliant on services provided by and through space assets. It is difficult to envision a modern world without effective and reliable GPS for innumerable commercial and military uses. Commercially, space-based assets enable instantaneous global communication; global media broadcasting, timely meteorological data; and commercial remote sensing. Militarily, space assets assure the provision of ballistic missile attack warning and intelligence gathering satellites provide difficult to replace warning, force assessment, and arms control verification data. While the role of undersea cables is indisputably critical to assure massive flows of data, space-based communications play a vital role in Department of Defense planning and operational concepts.

As the importance of space has grown, so has its attractiveness as a theater of military operations for peer nation-states, weaker states seeking to pursue asymmetrical strategies, and potentially some non-state actors who could seek to inflict temporary denial of space access for political or limited military goals. Since the United States is seen as being critically dependent on space assets for its military and economic prowess, it is generally assumed that a determined opponent would seek to negate at least some of the U.S. advantage in this realm. The consequences of losing, even temporarily, some of the U.S. space capabilities would be difficult to overcome and potentially catastrophic. As an example, the loss of GPS location and time synchronization data would fairly quickly affect the management of power grids and air traffic control, paralyze ATM and cell phone operations, and potentially significantly disrupt most, if not all, of the U.S. and global financial markets.[30] Similar negative scenarios can be envisioned for the denial of space services for all other areas of the economy and the military that depend on satellite-provided data.

A Machine Revolution

Over time, developments in science and technology and the defense-related capabilities from such developments have had a dramatic impact on the outcomes of military operations and the manner in which such operations have been conducted. One concept worth noting involves the disruptiveness of both mature and emerging technology. Rapid, revolutionary and novel scientific discoveries that diffuse quickly into the population and are adopted in unexpected, innovative ways can have the unanticipated effect of disrupting the status quo.

Advances in science and technology are sometimes unexpected and non-linear, and these are capable of triggering revolutionary changes in the way humans

In a relatively short time, the United States—and other able actors—could be well into a technological transformation even more profound than the information revolution. This transformation will be based on the convergence of information processing, biological sciences, and advanced manufacturing techniques. The result will be radically different approaches in the application of physical force against an enemy, as well as in the collection and processing of information.

[30] Hamblins, David, *"GPS Chaos: How a $30 box can jam your life."* New Scientist (web) 21:06, 06 March 2011.

adapt, manipulate, and control their environment. A review of existing developments in science and technology appears to support the hypothesis that the drive from the *Few, Expensive and Manned* to the *Many, Cheaper, and Unmanned* will underpin many of the technological breakthroughs that will contribute to future defense and security capabilities.

The key will be the evolution from unmanned to semi-autonomous to autonomous machines of war. We are already seeing in naval design the notion of the smart ship whose goal is to reduce significantly the crew size. This trend will continue into various schemes such as a mother ship with drones where a single human crew leverages technology and smart machines to control significantly larger robotic warrior units.

In a relatively short time, the United States—and other able actors—could be well into a technological transformation even more profound than the information revolution. This transformation will be based on the convergence of information processing, biological sciences, and advanced manufacturing techniques. The result will be radically different approaches in the application of physical force against an enemy, as well as in the collection and processing of information.

The trend toward miniaturization is already well under way in numerous research projects, many funded by the Defense Advanced Research Projects Agency. At the extreme are concepts like "fire ant warfare," with the battlefield dominated by large numbers of small semi-autonomous machines, networked together and capable of rendering an area impassable to troops or conventional mechanized formations.[31] On a more traditional footing, engineers have built small robotic devices to extend our reach on the battlefield or to search for IEDs.[32] Moving forward, there will likely be tiny unmanned aircraft, insect-like crawlers to carry sensors, and long-loiter high-altitude drones supporting ISR. It is taken for granted that such devices will be tied into U.S. battlefield information networks, and that they will be inexpensive enough to be used on routine missions, such as scouting in urban terrain.

As useful as these miniature devices are likely to be, they provide only a glimmer of what may be possible in the longer term. Rather than robots several inches in size, researchers are developing machines built atom by atom, measuring only a few nanometers (billionths of a meter) across. Such nanotechnology is in its early development stage, but holds much promise. The technology has moved beyond the basic research stage to producing remarkable advanced manufacturing techniques and molecular structural materials, and is likely to result in machines that are highly miniaturized if not actually microscopic.

Biotechnology has similarly been a topic of extensive interest, particularly in the wake of commercially successful efforts in the chemical and material industries (e.g., pharmaceuticals, high value intermediates, food and feed additives, bulk chemicals, lubricants, biofuels, structural-fibers, polymers, and composites) Much of the discussion has centered on therapeutic applications of genetic technology and on the ethics of procedures such as stem

[31] Originally suggested by Martin C. Libicki, The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon, McNair Paper 28 (Washington: National Defense University, 1994).

[32] http://www.army.mil/article/63473/Engineers_practice_using_robots_to_detect_bombs/

cells, genetic intervention to "cure" conditions, and human cloning. What has received less attention is the continued confluence of three driving trends--the synergistic merger of molecular biology, nanotechnology, and information technology, pointing to useful new directions in the design of mechanical devices.

Nevertheless, these seemingly positive trends are balanced by the various negative ramifications of these science and technology breakthroughs – namely, perverse applications of genetic engineering, designer bio-weapons, and other unanticipated products of improvisation and experimentation. Undoubtedly, unethical actors will be prepared to profit from unregulated aspects of science and technology; today's and tomorrow's adversaries will seek access to increasingly available emerging technologies that would undergird their efforts to harm or threaten U.S. interests.

Nanotechnology

Nanotechnology has diverse applications that will no doubt be a key enabler of future defense capabilities. Nanotechnology deals with matter at length scales below 100 nanometers – about the size of a virus. At that level, matter takes on unique characteristics and properties different from bulk matter. These include novel electrical, structural, and chemical behaviors that will enable the convergence with biological, material, electronics and cognitive sciences to produce unimagined capabilities in a broad variety of applications.

Still nascent applications will become important capabilities in the future: these include ultra-strong and light materials (i.e., for aerospace and transportation, uninhabited aerial or undersea vehicles), new power (battery) sources and harvesting technologies, ultra-efficient water purification systems, advanced weapons (including non-lethal), nano-electronics, small networked sensors, paper-flat organic nano-LED displays, advanced medical treatments, protection of communications/information systems, and inventions that are lighter, smaller, and highly energy efficient. According to *The Project for Emerging Nanotechnology*, their nanotechnology consumer products inventory contains 1317 products or product lines as of March 10, 2011.[33]

Various futures documents predict that defense applications of nanotechnology will see fruition by 2020, mainly in the area of electronics materials. In the coming decades, nano-devices such as nano-bots will emerge; in the defense context, these would be extremely small, swarmed, and autonomous machines. Other emerging applications may include miniaturized and affordable sensor suites, uninhabited combat vehicles, virtual reality training and education environments, augmented wound-healing compounds, highly adaptive clothing, and camouflage.

Biotechnology

Advances in molecular biology, pharmacology and the burgeoning biotechnology industries will facilitate the convergence of nano and biotechnology enabling targeted drug delivery, genetic

[33] http://www.nanotechproject.org/inventories/consumer/analysis_draft/

manipulation, in-vivo surgery, and advanced high-resolution medical imaging. In the coming decades, nanotechnology and biotechnology may even be able to modify human body chemistry without recourse to drugs to compensate for sleep deprivation and reduced alertness so as to enhance human performance and survivability.

Human age spans in wealthy countries will continue to lengthen because of the control of disease and the eradication of degenerative diseases. Projected quality-of-life improvements include bionic implants, organic/computerized prosthetics and organs, memory drugs, brain-machine interfaces, and a myriad of human performance enhancement technologies. Genetically modified foods will become widespread, which may have major positive repercussions on a global level with respect to climate change, population growth and changes in irrigation capacities and arable land.

Biotechnology applications will enhance the ability to wage war because of advancements in body protection and human performance. Soldiers will probably have access to real-time and transparent battlefield vital signs monitoring, rapid tissue healing, and full-spectrum drugs for protection, and treatments against designer bio-weapons and agents. On the other hand, a broader array of adversaries will also have access to new and emerging developments in biotechnology. Individuals, state-sponsored opponents, or nation-states will probably not only have the ability to design and insert new and highly virulent bio-weapon strains, but they may also have access to extremely effective delivery systems such as micro-uninhabited aerial vehicles. Such advances in technology should also enable better detection capabilities both for nano-materials and bio agents.

Additive Manufacturing

Additive manufacturing (AM) is the primary means by which states, non-state actors, and even individuals can acquire advanced technological designs and capabilities quickly and inexpensively. At scale, for nation-states, these capabilities foretell the introduction of the *Many, Cheaper, and Unmanned* paradigm, enabling a fundamental transformation of states' military capabilities.

AM refers to a process that builds up a component in layers, as opposed to a subtractive operation, which removes matter from a block of material to form a product. Increasing demand for customizable, quick turnaround, low cost products has opened the door for AM processes to enter the large scale production market once dominated by subtractive processes. Compared to AM, subtractive operations have relatively high capital costs and limited product design flexibility.

Additive Manufacturing is particularly useful where:

- Production volumes are relatively low,
- Part geometries are complex,
- Materials used are expensive, and/or
- Materials used are difficult to process by conventional means

Two types of AM highlighted in this paper are Powder-Based AM and Three Dimensional Printing.

Powder-Based Additive Manufacturing

Powder-based AM processes build layers of metallic and plastic materials by dispersing powders on a substrate. Similar to the liquid-based processes, the powder is then cured by an ultraviolet (UV) light source (usually a laser). Powder-based processes have found widespread use in the fabrication and repair of metallic components because of their ability to deposit metal on an existing substrate.

Electron beam melting (EBM) was developed in the late 1990s and is used primarily in the development of fully-dense, functional, metallic components. The EBM process uses an electron beam gun to create molten layers from metallic powder in a vacuum setting. Each cross-sectional layer is outlined according to a computer-aided design (CAD) drawing.

While the layer is still warm, the surrounding area is heated and the next layer of metallic powder is applied. By heating the surrounding area, the powdered particulate is sintered, preventing material repulsion and improving the material quality of the down-facing surface. With the ability to create fully-dense, metallic components EBM is used for the production of parts that require high strength properties.

As shown in Table 1 below, titanium and steel alloys are typically used for the EBM process, and thus it is ideal for the development of metallic components that have complex surface geometries. In addition, EBM can produce both thick- and thin-walled structures. This is ideal for applications, such as components for the aerospace and automotive industries, which require low volume production of thin-walled parts that possess the strength properties of titanium and steel alloys (e.g., landing gear). The ability to fabricate complex titanium components has also resulted in the use of EBM for the production of knee implants and bone plates in humans and animals.

Electron beam melting	
Superalloys	Stainless steels
Tool steels	Aluminum
Titanium	Copper
Laser Engineered Net Shaping™	
316, 304, 17-4 stainless steels	Nickel-based superalloys
Tungsten	Copper
Aluminum	M300 steel
H-13 tool steel	Titanium
Low alloy steel	Nickel aluminides
Selective laser sintering	
Polystyrene	Sand
Polycarbonate	Polyamide
Glass filled polyamide	Tungsten
Copper	Aluminum
Low alloy steel	
Inkjet/3D Printing	
316L stainless steel + bronze	420 stainless steel + bronze
Wax	Starch
Plaster	Molding sand

Table 1. Examples of additive manufacturing processes and materials
(Source: http://ammtiac.alionscience.com/quarterly)

Additive Manufacturing offers huge potential cost savings in production for the defense industry. It also enables designers to create completely new and innovative light weight designs using advanced lattice structures.

Three Dimensional Printing

3D printing (3DP), another example of AM, is a phrase used to describe the process of creating three dimensional objects from digital files using a materials printer, in a manner similar to printing images on paper. Developed in the late 1980s, 3DP is a process that uses an inkjet system to deposit a low-viscosity binder onto a powdered-material bed through the use of a pattern derived from a CAD model. Once the binder has dried, the completed part is removed from the machine and any excess powder is removed. Plastic components will usually be infiltrated

with a wax or epoxy resin after curing in order to improve the ability of the part to withstand mechanical stresses. Commonly used for prototyping, 3DP has gained popularity as a method of producing mold cavities for investment casting, and as a viable method of rapid tool production. In addition, 3DP technologies set themselves apart from other AM processes in that they can produce rigid, thin-walled parts. For example, printing systems like PolyJet Printing can produce parts with wall thicknesses of less than 1 mm. A wide range of 3DP applications is a direct result of the types of materials that can be printed (e.g., metal, plastic, sand, and wax). The ability to use wax and sand in the printing process has led to the creation of more complex mold cavities. Similar to stereolithography and laminated object manufacturing, these materials are less susceptible to the effects of thermal expansion during the development of a mold cavity than injection molded processes.

One example of using 3DP to create molded parts is the direct shell production casting (DSPC) process. In DSPC, a thin layer of aluminum is laid down with a roller and a silica binder material is sprayed over the aluminum. Once the layers are built up into a completed "green" mold, the mold is fired in preparation of accepting molten metal. DSPC has been used primarily in the development of engine components (e.g., intake manifolds, cylinder heads, and fuel injectors), but it can also be used to cast parts similar to those produced via investment or sand casting.

The closing paragraph in an Economist article last year captures the essence of the potential for this technology:

> "Just as nobody could have predicted the impact of the steam engine in 1750—or the printing press in 1450, or the transistor in 1950—it is impossible to foresee the long-term impact of 3D printing. But the technology is coming, and it is likely to disrupt every field it touches. Companies, regulators and entrepreneurs should start thinking about it now. One thing, at least, seems clear: although 3D printing will create winners and losers in the short term, in the long run it will expand the realm of industry—and imagination."[34]

New Energy Sources

In current efforts to build small, autonomous devices, one of the greatest obstacles is the energy supply. For example, while the robots used to clear IEDs are incredibly effective in their mission, their main limitation is in the power supply. The robot's batteries last about four hours, while route clearance missions can last up to 12 hours. Chemical fuels are too heavy, photo-voltaic systems do not produce enough energy, especially in low light, and batteries either weigh too much, or don't produce enough energy for long enough, or both.

Again, molecular biology may come to the rescue, as machines shrink small enough to be powered by the same biochemical processes that sustain living organisms. It may be possible to harness photosynthesis or other biochemical energy mechanisms to fuel manmade devices.

On a larger scale, development of new energy sources continues, driven primarily by market forces and past investments in exploration, infrastructure, surveying, extraction, refining, and

[34] The Economist, February 10, 2011, "Print me a Stradivarius: How a new manufacturing technology will change the world."

distribution facilities. This trend will continue, driven by the expanding industrial economies and energy needs of India and China. The relentless demand for fossil fuels will be sustained by existing and newly discovered oil stocks (e.g., oil sands) and their anticipated economic benefits. Towards 2030, however, new energy sources are expected to begin to emerge as they become more affordable to exploit.

Such sources include "low energy" nuclear fusion (cold fusion), solar, hydrogen fuel cells, tidal, and wind energy. In the commercial sector, there will likely be strong market incentives and the continuing introduction of environmental ("green") legislation for ensuring the maturation of advanced autonomous power sources: hydrogen fuel cells, renewable energy niche markets (bio fuels) and portable highly-dense energy-yielding technologies.

These will be supported by advances in other technology areas like carbon nano-tubes (which serve as small and efficient battery storage devices). Such technologies will have important applications and utility in meeting the requirements of the future soldier-borne technologies expected to emerge with the development of parallel convergent technologies. The battlespace will see the introduction of various lethal and non-lethal direct energy weapons including the possibility of mobile Electro Magnetic Pulse (EMP) devices. The soldier of the future will also require continuous, portable, lightweight, and high-output energy sources to power such items as active/passive camouflage garments, C4, medical monitoring, sensing, robotics, and weapons applications.

Cognitive, Behavioral, and Social Sciences

Efforts to understand the human mind (both culturally and physiologically) will lead to some dramatic breakthroughs in defense and security capabilities. Corresponding advances in computing will underpin the future of the cognitive sciences, a situation that arises from the computationally intensive nature of exploring the complexities of the human brain. It will become possible to do mathematical mapping of social networks, which will combine advances in computing with clearer insights into human motivation, intent, anthropology, and humans in social groups. Advanced neuron-imaging techniques will afford precise localization of cognitive functions mapping, a process that will enable a plethora of capabilities, including seamless brain-machine interfaces, instantaneous language translation, and accelerated learning technologies. Synthetic intelligence will accordingly become feasible for many applications by 2030 (including autonomous combat vehicles in all environments), and the ability to predict adversarial intent will become possible. Advances in the cognitive, behavioral, and social sciences will have moral, ethical, and legal implications and will pose significant policy challenges for all nations.

Human Augmentation

Human enhancement refers to the intent to overcome temporarily or permanently the current limitations of the human body through artificial means. The term is sometimes applied to the use of technological means to select or alter human characteristics and capacities, whether or not the alteration results in characteristics and capacities that lie beyond the existing human range. Here, the test is whether the technology is used for non-therapeutic purposes.

In 2010, an exoskeleton project run by the Defense Advanced Research Projects Agency (DARPA) had produced some promising technology. According to *Network World*, this system, which weighs about 55 pounds, can enable human operators to carry 200 pounds with little or no effort resulting in far less fatigue. Other exoskeletons systems under development can run at speeds of 10 miles per hour and perform squats and crawls, in addition to lifting.[35] These exoskeletal machines are also equipped with sensors and GPS receivers to assist soldiers in obtaining information about the terrain they are crossing and how to navigate their way to specific locations. DARPA is also developing computerized fabrics that could be used with the exoskeletons to monitor heart and breathing rates.

Developing powered exoskeletons may also provide a huge benefit in non-military applications as well, since the technology can improve the lives of people with spinal injuries or disabling neuromuscular diseases. For example, a company called Berkeley Bionics is testing eLegs, an exoskeleton powered by a rechargeable battery, which is designed to enable a disabled person to walk, to get up from a sitting position without assistance, and to stand for an extended period of time.[36]

Warriors have been wearing / using mechanical means (e.g., armor) to protect and improve the effectiveness of their bodies in battle since ancient times. It is reasonable that this trend will continue into the future, but the issue of human augmentation faces stiff resistance in certain ethical and religious spheres. DARPA ran into serious public relations troubles with its programs in this area, but the promise of improvement and optimization are very strong.

Bringing it Together…

All this begs the question: What does it means to "fight" in a globalized, highly interconnected world where the barriers to entry for significant military engagement are relatively low?

Globalization and the related cyber connections change the definition of borders – including space. Separation distance moves into a paradox: interconnectedness brings things closer network-wise, but automation, robotics and the machine revolution separate adversaries even more because the element of human fear on the battlefield is removed or reduced. In addition, there is a new factor to address - the ability to maneuver virtually, with no actual movement in the battlespace. In this setting, all 'action' is through information. Finally, using the standard military measures of Mobility, Survivability and Lethality, conventional wisdom has been that these three factors make up the trade space for force considerations. To improve in one measure typically took something away from the other two. But with a move from the *Few, Expensive and Manned* to the *Many, Cheaper, and Unmanned* paradigm, it becomes possible to improve all three simultaneously. For example, due to advances in small robotics, designers can now have both mobility and lethality (instead of making a trade); and due to the low cost and unmanned aspects, survivability is a non-factor. With these trends in mind, the battlefield and character of war in 2035-2050 will be distinctly different from today,

[35] http://www.networkworld.com/community/node/57992

[36] http://berkeleybionics.com/exoskeletons-rehab-mobility/about-elegs/

threatening the warrior ethos of the military. At the very least, this new environment will require redefining the warrior ethos and culture.

Against the backdrop of the future security environment depicted here, the ensuing chapters examine the future characteristics of conflict in 2035-2050, the nature of future competitions in that timeframe, and what constitutes an impending Renaissance in Strategic Warfare.

IV. The Characteristics of Conflict in 2035-2050

"Conflict is inevitable, but combat is optional."

--- Max Lucade

As presented in the preceding chapter, global trends support a presumption of increasing instability and a growing possibility of confrontation and conflict in the 2035 to 2050 timeframe. The inter-connecting effect of globalization will continue to accelerate the pace of change in the character of conflict, and access to resources (energy and non-energy) will likely drive the security interests of nation-states. Ultimately, control over these resources and their methods of distribution through the available lines of communication will be a critical feature of conflict. In fact, issues of control and distribution may become prime-movers for why, where, and, thus, how the United States fights.

It is also reasonable to accept that state failure will continue to be a dominant feature of future conflict. Application of whole of government or "smart power" approaches that integrate the full range of governmental capabilities may assist in preventative measures for state failure, and may help mitigate the more severe consequences of state failure if the military instrument is used as an integrated element of a national response.

A central premise of this paper's vision of the nature and character of warfare in the 2035-2050 timeframe is that the number of actors (state and/or non-state) that can operate at the strategic level on the world stage is increasing, while the technological barriers to developing credible threats are dropping, thus creating a very complex environment within which the United States must operate. Since the end of the Cold War, more nation-state and non-state actors have emerged; in the future, there will likely be many more actors than there are today. While many new actors are small-to-medium size, they will have the ability to operate against larger actors at the strategic level of war in a far greater variety of ways than they could historically due in large part to the trends described in the previous chapter. Thus, smaller actors (e.g., Somalia, Yemen, and Hamas) that today have relatively limited options by which to influence the strategic decisions of larger actors (e.g., US, China, and UK), will be able to do so in a range of new and emerging ways in the coming decades.

A diverse and expanding set of actors, especially non-state actors, already frequently operate covertly or as proxies for nation-states. Non-state actors are not bound by internationally recognized norms of behavior, and they are resistant to traditional means of deterrence. Extremist non-state actors, typified by al-Qaeda and its associates, are likely to remain a significant threat to the United States and its allies.

These non-state actors will continue to contribute to an increasing set of *hybrid threats* – dynamic combinations of conventional, irregular, terrorist, and criminal capabilities. They make pursuit of singular approaches ineffective, necessitating innovative solutions that integrate new combinations of all elements of national power.

This chapter provides a series of illustrative examples of conflicts in the 2035-2050 timeframe. These examples include various types of actor-on-actor conflicts (involving state and non-state actors of various sizes) that could emerge and describes the nature of the military and/or technological competition around which such conflicts will focus.

The Range of Actor-on-Actor Conflicts (*and Engagement*)

The word "conflict" is used rather than "warfare" because a conflict can occur in a number of ways between actors, some of which do not include direct military confrontations or clashes. In some ways, war has become a reserved term for the way nation-states settle differences with their militaries. In the future, with many more players at the strategic level, war will be but one means of interaction between militaries. Thus, conflict can be seen as a more comprehensive set of conditions that takes place along a continuum between times of peace or in times generally viewed as "war."

Future conflicts will occur between state actors, between state and non-state actors, and increasingly between rival non-state actors. We have already seen a number of examples across this spectrum in recent years: from the U.S. invasion of Iraq in 2003 and subsequent insurgency to open hostilities between Israel and Hezbollah in 2006 to Israel and Hamas in 2008. An example of non-state actor conflict is Hamas and the PLO fighting for control of Gaza in 2007, with Hamas emerging victorious. Figure 6 shows the range of potential future conflicts which the United States must be prepared to address.

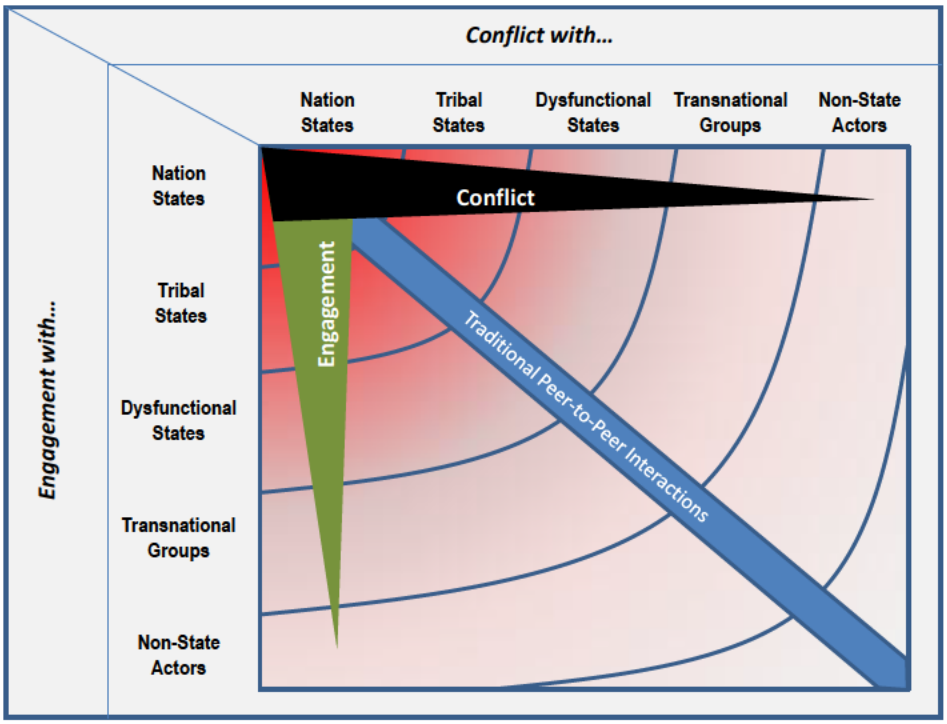


Figure 6: The Changing Face of Conflict in an Interconnected World

(Source: Booz Allen Hamilton)

As indicated in the figure above, nation-states need to acknowledge that they will be in officially-recognized conflict with many more types of actors in the future. There are many factors that determine the structure of competition in the environment of expanding globalization. Since a nation-state's military is a reflection of the economy that produces it, then the factors that define the economy directly influence the nature of its military. These economic factors, which dominates the nature of military competitions, include the price sensitivity of particular industries, ease of entry for new participants, the bargaining power of customers and suppliers, and the threat of substitute services or products. Hence, competition will continue to be core basis for the interaction among actors in the international arena. However, collaboration at a strategic level across the spectrum of international actors will likely take on a similar role. Stated another way, the highly interconnected and converged world of the future will mean that these new actors can represent a new source of positive engagement as well.

In the future, the concept of allies will have much more of a business/industrial feel to it than we current see: competitors on one issue may be partners on another. While this is not a new concept, extending it outside the 'club' of nation-state to all actors on the continuum will be quite new, and challenging.

Future conflicts will involve a range of transnational, state, group and individual participants who will concentrate and operate both globally and locally. In some conflicts, there is likely to be concurrent inter-communal violence, terrorism, insurgency, pervasive criminality and widespread disorder. This again will call for a "smart power" response on the part of the United States. However, the tactics and techniques of U.S. adversaries will rapidly adapt to counter the smart power approach and ultimately strive to gain advantage and influence through economic, financial, legal and socio-cultural means. These forms of conflict are transcending the conventional understanding of what equates to irregular and regular military activity. Truly adaptive adversaries will also seek to play U.S./Western media and political systems to their advantage and they will adjust their tactics accordingly.

Hierarchical Levels of Military Activity

Before examining the range of strategic options that will be available to adversaries in the coming decades, it is necessary to review briefly what is meant by "strategic" level actions.

In general, one can characterize military activity, including the activity that characterizes a military competition between state and/or non-state actors, as taking place within five different hierarchical levels. The levels are:

- National policy
- Strategic
- Campaign
- Operational
- Tactical

Each level is described briefly below. These levels are not absolutes, but rather a reflection of what has emerged as traditional Western thinking about military actions. Moreover, the boundaries between the various levels are not nearly as precise as the following descriptions might lead one to believe. The boundaries between the levels could easily be as indistinct and hazy as they are precise and well-defined, depending on the nature of the actions and the lines of authority established by the military force in question. Nevertheless, the use of the levels enables us to demonstrate the increased ability of smaller states and non-state actors to shape the international environment at the strategic level.

National Policy

Overall national security policy is set by the political leadership of a state actor or, increasingly a non-state actor's leadership. The leadership (which could be a democratically-elected civilian government or a military regime) determines the priority threats and overall strategic objectives of a conflict or peacetime military competition based on the "national" interests of that actor. Once the political leadership determines the national-level policy guidance, the military leadership uses the guidance to shape its strategic planning and forces.

Strategic

The strategic level refers to plans created by the military leadership in support of coordinated efforts to execute national policy using all instruments of power and influence.[37] In other words, the national leadership's political objectives, once established, are the starting point for developing strategic military plans and forces necessary to achieve those political objectives. These strategic plans can be developed for peacetime competitions; for conflicts that do not reach the threshold of what is traditionally considered as "war" between actors; or for armed hostilities between competing actors that is generally held to be a state of "war" by the participants.

Campaigns

A campaign is a sustained series of military operations designed to defeat the enemy's forces in a specific space and time, with simultaneous and/or sequential battles. Usually, several campaigns are required to achieve the desired strategic objectives established by the actor's political leadership. Thus, the successful execution of a larger strategic plan is accomplished through the sequential and/or simultaneous conduct of a variety of campaigns. Campaigns can be characterized in a variety of ways, such as ground, air, naval, space, cyber, and undersea. At the campaign level of war, the *theater of operations* is the region where specific campaigns and their supporting operations are conducted. As largely cyber-centric campaigns are employed, the theater of operations of a conflict expands to include the domain of cyberspace.

[37] It is at the strategic level where, historically, there has been the greatest tension between the civilian leaders that set a nation's policy objectives and the uniformed military responsible for developing the strategic military plans intended to achieve those policy objectives. History, particular in the United States, is full of examples of generals (McClellan in the Civil War, MacArthur in the Korean War) that have chafed under the constraints laid down by their political masters. In another example, many observers, especially those in the uniformed military, have been inclined to blame the U.S. defeat in Vietnam on America's civilian leadership and the overly political restrictions placed on the war's strategy.

Operations

Major military operations consist of a series of tactical actions, battles or engagements sequenced and synchronized to accomplish a larger campaign objective. As with campaigns, operations can also be classified as ground, air, naval, amphibious or space. In the future, various types of cyber operations will make up the elements of a cyber campaign.

Throughout the history of warfare, new technologies and "machines of war" are generally unveiled first at the tactical and/or operational levels. However, their success (or failure) at the tactical level will likely spread up through the other levels rather swiftly, as leaders come to grasp the strategic implications and possibilities offered by employing these new technologies.

Tactics

The tactical level refers to the specific techniques combat units use to fight battles or engagements to secure a specified operational objective. At the tactical level, it is in the *combat zone* that these engagements or battles are fought. Again, the employment of cyber weapons or concepts that increasingly rely on semi-autonomous or autonomous machines will have a major impact at the tactical level as well as the campaign and operational levels.

Throughout the history of warfare, new technologies and "machines of war" are generally unveiled first at the tactical and/or operational levels. However, their success (or failure) at the tactical level will likely spread up through the other levels rather swiftly, as leaders come to grasp the strategic implications and possibilities offered by employing these new technologies.

Each of the levels described above is also characterized by different actions, procedures, and goals. Moreover, each level of military activity consists of numerous, simultaneous and interdependent tasks that military organizations must execute with differing levels of intensity to perform with proficiency. These tasks include procurement, planning, training, logistics, intelligence, technical adaptation and combat. Especially into the future, technical adaptation will include the introduction and widespread adoption of robotics and autonomous systems. As non-state actors such as Hezbollah and Hamas have found in recent years, they too have to address these levels of activity if they desire to maintain some form of military power.

The representative conflicts presented in this chapter focus initially at the strategic level of engagement and military activity to highlight the likely interactions between actors in the 2035-2050 timeframe. The interactions will, of course, be more complicated and richer in context than can be presented here due to space limitations. For each of the illustrative conflict scenarios depicted, this chapter addresses the following overarching questions:

- What is the strategic context of the conflict?
- What is the nature of the competition?
- What are some of the strategic-level actions/options available to the actors involved?
- What are some of the major campaigns that would be conducted during the conflict that are central to achieving an actor's desired strategic objectives?

- What are some of the key operations that would have to be conducted during those campaigns?
- What force capabilities and/or requirements would be most desirable for those operations and/or campaigns?

Illustrative Future Conflicts

Each epoch of warfare is marked by its specific characteristics which make it unique. In the period in question the development of warfare will be primarily shaped by growth in the capabilities of strategic communications, cyber warfare, and space warfare, as well as the growing potential for surprise attacks by "5th column" electronic saboteurs and a growing reliance of discreet but highly effective SOF-like strikes. These developments will result in warfare far different from the past - one without front lines, major campaigns traceable on media maps, or a distinction between the battlefield and the opponent's heartland. States, which would be traditionally judged as not militarily significant, have the potential to use these new capabilities to attack a more powerful opponent's center of gravity literately over and through his formidable, deployed armed forces. Even more unsettling is the potential for non-state actors and even individuals to selectively but highly effectively attack key values of a nation state in order to achieve specific political or social goals.

Armed struggle is likely to be more focused on issues involving valued natural resources and over disputed territorial claims, which given their frequent intersection, suggesting a heightened future probability of conflict at sea. Consequently, not only the South China Sea but the progressively more ice-free Artic will become more important for both planning and for actual operations to achieve national goals. Availability of minerals (which may not be ipso facto scarce but may be limited by economic factors to a few production sites), which are vital for high technology devices, may be another source of conflict resulting in military operations to force a "fair" distribution of the prized material. On a different plane, a non-state actor may elect to attack a militarily powerful nation-state through a cyber-attack to undercut the legitimacy and thus the popular support of its opponent, with the hopes of furthering a specified political objective. Finally, *tribal* and *dysfunctional* states (and some long-established non-state actors), unable to create formal military establishments, may elect to engage each other using specialized irregular forces which would mimic (but not equal) Special Forces units of the established powers.

The world of 2035-2050 will see a wider range of conflicts than today as more and more actors (state and non-state) emerge to act on the world stage, and exploit the strategic opportunities afforded by technology trends and changes in perceptions of sovereignty. The illustrative conflicts described below could occur between any of the actors that will be on the world's stage in the future security environment, from large nation-states in conflict against religiously-motivated non-state actors, to tribal states competing against each other, to rival transnational groups potentially aligning themselves with one nation-state against another.

These future conflicts will revolve around one or more military and/or technological competitions that are central to the fundamental character of the individual conflict. Some of

these future competitions will be explicitly military in nature, such as the current one characterizing the anti-access/area denial competition between the United States and China in the Western Pacific. Other competitions will be a mix of military and non-traditional elements, such as increased use of special-operations-like forces employed by both state and non-state actors. Such forces do not necessarily have to belong formally to the military, as evidenced by the American CIA's use of drones and its own SOF-like units in Yemen and Afghanistan. And other competitions will have virtually no overt military component to them: these could include (but are certainly not limited to), the use of international law to pursue a major policy objective or leveraging existing and future types of social media to influence the views of populations.

This chapter posits five illustrative conflict scenarios:

1. A conflict involving substantial naval combat in and around the South China Sea. The central competition, or campaign, in this scenario is a future variation on today's Anti-access/Area-denial (A2/AD) competition;
2. A conflict involving substantial combat in the Arctic. The central competition in this scenario also involves a variation of today's Anti-access/Area-denial (A2/AD) competition;
3. A conflict over a valuable resource critical to the continued health of the world economy. The central competition of this conflict is "commodity access denial;"
4. A conflict where the central competition involves a physically-destructive cyber campaign; and
5. A conflict where the central competition involves the ability of opponents' respective "special operators" to influence the outcome of the conflict. (This scenario could also be between two nation-states that decide to confront each other with "Special Operations" forces rather than traditional military force units.)

However, there are two, overarching competitions in play today that will continue to be a factor in the future security environment, and will influence to varying degrees all four of the illustrative scenarios described below. They are (1) the strategic communications competitions that take place at the national, regional and international levels, and (2) the competition to limit the proliferation of weapons of mass destruction (WMD).

Strategic Communications

In different eras, the strategic communications competition went by a variety of names, such as the propaganda war, or disinformation campaigns. In 2003, the Chinese Communist Party endorsed "media warfare" (the use of various communications media to influence domestic and international public opinion during a conflict) as one of the three new "warfare concepts" to be adopted by the People's Liberation Army (PLA).[38]

[38] In addition to Media Warfare, the others were Psychological Warfare (deterring, shocking and demoralizing enemy personnel) and Legal Warfare (using international and domestic law to gain international support). See Office of the

Regardless of the name, this competition is about which actor(s) will have dominant influence over the strategic narrative. Put another way, which actor's version or vision of what is best for its nation, the region, or the world will be the dominant one—the one that garners the most local, regional and international support. Whichever side's narrative emerges as the dominant one is the side that will very likely have the greatest degree of popular and/or political support.

Throughout recorded history, virtually every instrument of communications has been enlisted in the struggle to achieve the dominant narrative. The printing press, radio, movies, and television have all been used in this competition. Today, these traditional tools of strategic communications have been complemented, perhaps even surpassed, by the wide range of social media unleashed by the power of the Internet. Today, social media such as Facebook, YouTube, and Twitter, are credited with shaping the narrative as well as world events in examples such as the Arab Spring and domestic unrest in China. Whereas Western media outlets (such as the BBC or CNN) tended to dominate the international airwaves in the recent past, they have been joined by competitors such as Al Jazeera (which broadcasts internationally in both Arabic and English).

Just as no one could have predicted ten years ago the types of social media and associated technology that are playing such a dominant role in the battle for the narrative today, it is impossible to predict what the new tools of strategic communication will be twenty to thirty years from now. One thing is certain, however. Just as nation-states and non-state actors will strive to harness the potential of these tools to prevail in the competition for the narrative today, the multiplicity of such actors will do so in the future.

The Proliferation of Weapons of Mass Destruction (WMD)

Chemical, biological and/or nuclear weapons have been a major factor in either the planning or execution of conflicts for nearly a century. The proliferation of such weapons, the technology to develop them, and the means to deliver them has been a major concern since the end of the Cold War. The list of countries that possess nuclear weapons is growing, and there is every reason to believe that more state actors will possess them in the future. The presence of WMD in a region (particularly nuclear weapons) changes the security and decision calculus of the region's leaders. While it is likely that traditional nuclear deterrence will hold between nation-states that possess nuclear weapons, there is a growing concern that possession of WMD (particularly nuclear weapons) by *tribal* and *dysfunctional* states increases the chances that such weapons could fall into the hands of dangerous non-state actors or other nation-states that may not subscribe to the traditional notions of nuclear deterrence. To prevent this eventuality, larger states will be compelled to develop contingency plans to secure or destroy those weapons.

The prospect of unsecured, "loose" nuclear weapons, particularly in a region with significant non-state actors comprised of extremists, could trigger the emergence of what could be called

---

Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010,* Washington, D.C, 2010, p, 26.

an era of irregular nuclear warfare. The use of even one or two nuclear weapons by extremists or a non-state actor against the United States homeland raises the critical question of what would be the tipping point when the United States would also consider the use of such weapons. Perhaps more vexing is the question against whom should such weapons be used? Contending with the loose nukes challenge in a nation-state dominated world is hard. Contending with loose nukes in a multi-dimensional, multi-actor world will be exponentially harder.

The Anti-Access Conflict of 2050 – the South China Sea

Contemporary discussions that address the anti-access/area denial (A2/AD) competition between state actors largely focus on a small set of scenarios (e.g., Taiwan, Iran). The contemporary A2/AD competition between China and the United States is focused around the long-range precision strike systems that China is developing to counter the traditional, large platforms (in particular aircraft carriers) associated with U.S. naval power projection. The current generation of big-deck, nuclear-powered American aircraft carriers represent the *Few, Expensive, and Manned* platforms being challenged by China's emerging A2/AD systems: such as anti-ship ballistic missiles, anti-ship cruise missiles, mines, and conventional submarines, which provide examples of the *Many, Cheaper, and Unmanned* paradigm.

But this current A2/AD competition is highly scenario-dependent, as the Chinese A2/AD systems, for the most part, are being explicitly developed to counter the intervention of the United States in the event of a conflict with China over the future status of Taiwan. While some of these emerging A2/AD systems have relevance in other scenarios, their potency against major U.S. platforms may not be as potentially decisive as in a Taiwan scenario. Still, the A2/AD capabilities will remain formidable threats to any *Few, Expensive, and Manned* platform that dares to venture within range of them.

However, more varied anti-access scenarios are likely to emerge in the future security environment, particularly as the anti-access technology of today proliferates to more and more actors. Future anti-access scenarios could involve, for example, a conflict over energy resources (potentially in disputed territories) that are either focused at acquiring the resources by force, or denying an adversary the ability to exploit them. As more and more energy (particularly oil and natural gas) is increasingly extracted from the maritime domain (either in clearly defined and recognized territorial waters or in seas where national claims are in dispute), the extensive and expensive infrastructure necessary to exploit these resources will likely become targets for a potential adversary during a conflict. Moreover, the focus of a future conflict does not necessarily have to be around control and/or access to these maritime energy resources – the conflict could be over some other, totally unrelated issue, but the vulnerability of an actor's offshore energy infrastructure will make it a center of gravity that an adversary will almost certainly threaten during war as one of the major campaigns waged during that conflict.

The Scenario

For this scenario, the conflict is between two major nation-states over control of a major international waterway, specifically the South China Sea. This could still be categorized as an "anti-access" scenario as it envisions large-scale, force-on-force conflict between major state actors that are military peer competitors. Such a scenario could involve the United States and China, and/or another major power in the Asia-Pacific region, such as Indian or Japan. As a large conflict between major nation states, it will include virtually every element of traditional national power as well as emerging ones that have been examined in this paper, including physically-destructive cyber and "special operator" attacks against targets in the homeland. Thus, these major nation-state conflicts will also be wars without fronts, where the "homefront" is just as likely (and vulnerable) to being attacked on the first day of the conflict as any military forces deployed on the so-called "front lines."

As this scenario focuses on energy infrastructure in the maritime domain, naval warfare capabilities will be at the heart of this future competition. The traditional roles of naval power have been to either to maintain sea lines of communications (SLOCs) or to interdict them. These roles have been generally accomplished by a variety of naval missions, such as coastal defense, sea denial, sea control, and maritime power projection. These missions, moreover, can be conducted either sequentially or simultaneously. In addition, the force requirements for these missions can vary depending on the maritime geography, the scope of the SLOCs to be maintained and/or interdicted, and the technological capabilities of the respective adversaries.

In the 2035–2050 timeframe a potential competition and/or conflict for maritime dominance in the South China Sea region is likely – either as the cause of a conflict, or one of the campaigns within one. It could be the United States, as an element of a larger conflict with China, seeks to hold at risk something China values very highly, specifically its growing sea-based energy infrastructure in the South China Sea. Many Chinese energy analysts believe that the equivalent of Saudi Arabia's oil and/or natural gas supply could lie below the bottom of the South China Sea; an energy bonanza that China would likely reap given advances in energy extraction technology and the prospect of a some sort of political accommodation with Taiwan that enables China to exploit a greater portion of the South China Sea's energy potential than it currently can today. And this would be an energy infrastructure (along with the SLOCs that sustain that infrastructure and transport the energy resources it extracts from the South China Sea to China) that a potential adversary could hold at risk in the event of a crisis or conflict with China. By holding this energy region at risk, China's adversary could deter China from threatening other, lesser actors in the region. The key for any potential future adversary of China is to develop a naval force that can credibly hold at risk China's energy assets and SLOCs in the South China Sea for a sustained period of time, while still possessing the characteristics and capabilities that mitigate the risks posed by China's A2/AD systems.

The Campaign

A potential future campaign against Chinese South China Sea-based energy resources, infrastructure and SLOCs would consist of a number of inter-related operations, with the three key ones summarized below.

China's future adversary would need to conduct a series of **long-range, precision strike operations** against fixed sea-based energy infrastructure, such as oil and/or gas platforms, pipelines, pumping stations, and loading docks. The strikes could be launched from a range of sea-based and/or land-based sites, but their shared characteristic is a long-range that enables the launch sites to operate outside of China/s A2/AD envelope.

The adversary would also need to execute a series of **sea denial operations** against tankers and the vessels used to sustain the off-shore energy infrastructure. The spread of offshore energy facilities signals a new way of thinking about sea control and sea denial. Traditional views on sea control/denial tend to concentrate on China's commercial and/or naval vessels. With the increased importance of sea-based energy, the ability to deny China access to that energy introduces a new element to discussions about the future role of naval power in safeguarding (or attacking) that sea-based energy.

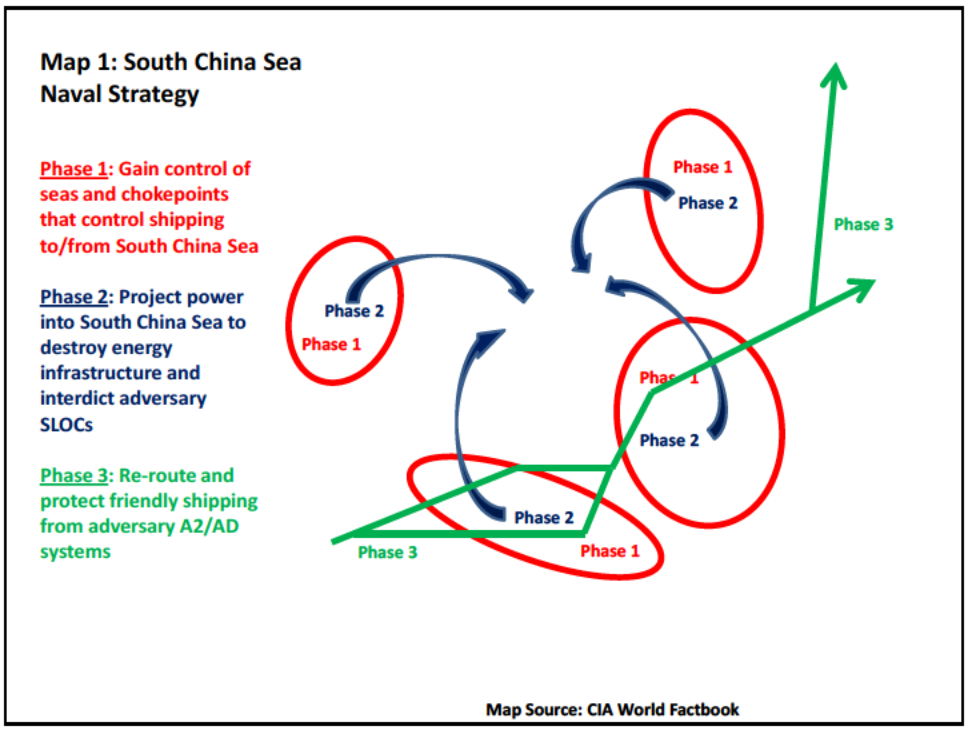
China's future adversary would also need to conduct a series of **supporting C4ISR/cyber operations** to ensure persistent pre-conflict surveillance of China's off-shore energy facilities as part of the campaign's larger targeting process. Moreover, China's adversary would also require near-continuous battle damage assessments of those facilities to monitor attempts to repair them and determine if addition strikes were required. These supporting C4ISR operations would be required for the duration of the campaign.

How the Campaign Would Play Out

During the pre-conflict period, China's adversary would likely seek to deploy and/or posture its naval forces either to deter China from considering aggression or to be prepared for immediate combat operations if deterrence failed and hostilities commenced. These naval forces, if provided with sufficient long-range weapons and endurance, would not need to be deployed into the South China Sea in order to threaten Chinese sea-based energy assets and facilities. They could hold those assets at risk from deployment areas in the Indian Ocean, from patrols areas south of Indonesia, or from the Western Pacific in the waters to the east of the Philippines.

The pre-conflict period could last indefinitely, which places an emphasis on a force with high, sustained endurance and a significant weapons payload to make deterrence credible. This future naval force would also require the connectivity to enable it to operate as an integrated force that can detect, identify, track and, if necessary, attack a range of maritime targets and threats. China's future adversary would deploy naval forces to positions within strike range of Chinese sea-based energy facilities and infrastructure, but outside the range of Chinese A2/AD strike systems.

Once naval forces have been deployed and are in position to conduct combat operations, the naval campaign against Chinese energy facilities and SLOCs in the South China Sea would unfold in three general phases (see Map 1 below).



Map 1: South China Sea Naval Strategy

(Map Source: CIA World Factbook)

Phase 1 of the campaign would focus on gaining control of the seas and littoral areas that guard the approaches to the South China Sea. Much of this Phase would likely be conducted during the pre-hostilities period. But after the start of hostilities, lethal force could be employed against any Chinese shipping bound to or from the South China Sea. The emphasis in this Phase would be to choke off China's commercial maritime traffic while mitigating the risk posed by China's A2/AD systems to friendly naval forces. It would be in Phase 1 that China's adversary could expect to receive the valuable support of allied naval units, such as those of Australia, Japan, India and/or the United States. China's ability to maintain its sea lines of communication would be at its weakest outside the South China Sea, and any naval units that China might have deployed in these waters in an attempt to protect those SLOCs should not present a significant challenge to the naval power of China's adversary and its allies.

During Phase 2, which could be conducted simultaneously with Phase 1, sustained volleys of long-range precision weapons (many of which could be launched from naval units also conducting Phase 1 operations) would strike key Chinese sea-based energy assets. The strike campaign could be planned to target most, if not all of these assets in a single wave of strikes. Or, they could be conducted in bursts as part of a larger attempt to coerce China to cease

hostilities or risk an escalation of the strikes that threatens to destroy all of their energy assets in the South China Sea. China's future adversary must be able to conduct this campaign until the larger conflict is over, or until there are no more Chinese energy assets left to threaten in the South China Sea.

Another key facet of Phase 2 would be interdicting Chinese SLOCs within the South China Sea. While long-range precision strikes could also be employed against Chinese commercial shipping in that Sea, other, traditional tools of naval power would also be utilized. These would include, but are not limited to, attack submarines (either nuclear-powered or equipped with advanced conventional propulsion systems) using either torpedoes or anti-ship cruise missiles to attack commercial and naval ships, and mines deployed from submarines and aircraft (manned and unmanned). The energy potential of the South China Sea is enormous, and in this scenario it is presumed that the energy derived from the South China Sea has become one of the leading energy sources (if not the leading energy source) for China. Thus, even the partial interdiction of the energy SLOCs in the South China Sea could place substantial economic pressure on the Chinese economy, society, and leadership, particularly when combined with the destruction of the facilities used to extract that energy from the South China Sea.

Throughout the conflict, allied and friendly commercial shipping that normally uses the South China Sea would have to be re-routed away from the conflict area and defended against any attempt by China to interdict it. Thus, Phase 3 (the re-routing and defense of friendly commercial shipping) would likely be initiated during the pre-conflict period. As with Phase 1, this would be an element of the campaign where allied naval forces could be employed to escort friendly commercial shipping, therefore allowing the main naval forces of China's adversary to concentrate on Phase 2 and the projection of power into the South China Sea.

In the post-conflict phase, China's adversary would desire to retain some forces in the region in order to convince the Chinese that a resumption of the conflict would involve immediate re-attacks on their surviving South China Sea energy facilities and the renewed interdiction of their SLOCs. As with the conflict phase, the post-conflict phase would likely be of an indeterminate length, again placing an emphasis on forces with high endurance, survivability and a high weapons volume.

Force Requirements

China's future adversary must be prepared to conduct an anti-sea-based energy campaign for the duration of any larger conflict, whether it lasts thirty days or thirty months. The forces required to conduct an anti-sea-based energy campaign in an A2/AD environment would comprise one element of the larger total force. However, the forces that would conduct a sustained anti-sea-based energy campaign would likely require a range of characteristics and/or capabilities. These include, but are not limited to platforms with high endurance and sustainability, including minimally-crewed or unmanned platforms; the ability to defends themselves and continue to operate effectively in a high-threat environment; platforms with

large weapons payloads; weapons with long-range precision strike capability; and a C4ISR/cyber network for continuous, sustained monitoring of the adversary and all other potential threats.

The United States (if it elected to) could exploit a range of emerging technologies to turn the current naval warfare competition on its head, not only in favor of the United States, rather than the current situation that, arguably, favors China, but also to evolve to a force that possesses most of the characteristics and/or capabilities cited above. For example, as the robotic/unmanned revolution continues, any power with a modest shipbuilding capability will be able to build many relatively inexpensive, lightly (or remotely) manned vessels capable of carrying hundreds, if not thousands, of long-range, expendable precision strike weapons that could threaten China's South China Sea energy resources at ranges outside those of China's emerging A2/AD systems. Moreover, these expendable precision strike weapons would have significantly greater ranges than today's manned strike platforms, and they could conduct a variety of missions, such as strike, ISR, and anti-submarine warfare.

Thus, the large, very expensive, heavily manned aircraft carriers of the present could be replaced by remotely-crewed, cheaper vessels that employ simple power drives with expendable precision strike weapons; these weapons would also be less expensive than the manned tactical aircraft currently flying from carriers today.

While an aircraft carrier would still be viable in this *anti-sea-based energy campaign* scenario against Chinese A2/AD systems (so long as it launched its manned aircraft while out of range of these A2/AD systems), it would be far more cost-efficient to use the *Many, Cheaper, and Unmanned* ships/weapons combination than the legacy *Few, Expensive, and Manned* aircraft carrier.

Moreover, it is feasible that some of these remotely-crewed large strike vessels could be submersibles or semi-submersibles, which would complicate an adversary's detection and targeting systems that support the long-range precision strike weapons. The shift to such semi-submersibles would confound and confuse the C4ISR network developed specifically by the adversary to target the large surface vessels (carriers) that characterize the current A2/AD competition.

The Anti-Access Conflict of 2050 – the Arctic

The Arctic is one of the world's least explored and last wild places. The total number of people that live above the Arctic Circle is estimated at barely four million, but the region possesses resources that could provide energy and raw materials for many millions more for years to come.

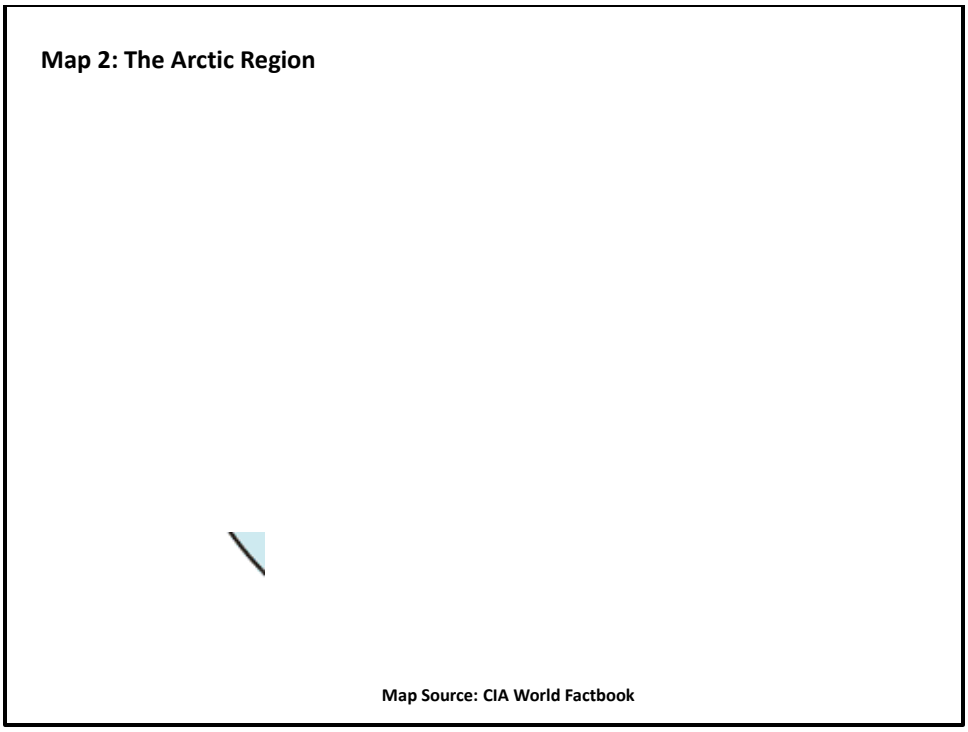
The Arctic, despite what many may believe, has been a theater of significant military competition. During the Second World War, it was the site of ferocious convoy battles that involved virtually every weapon that could be employed – submarines, mines, long-range land-

based reconnaissance/strike aircraft, aircraft carriers, and major surface combatants. For most of the second half of the 20th century, the Arctic, as the shortest route between the United States and the Soviet Union, was a likely theater for war, with conventional and/or nuclear weapons. The region was the main operating area for scores of nuclear-powered submarines and bombers operated by both the United States and Soviet Union.

The risks of future conflict in the Arctic over energy resources, however, may be exaggerated, as the development of these resources will likely be conducted in internationally recognized territory of sovereign actors, and likely as joint commercial ventures by a range of state actors and international energy companies. However, as with the South China Sea scenario described above, while future conflicts or major wars may not be *about* the Arctic, they could very likely spill over to *include* the Arctic. Future adversaries may seek to threaten each other's Arctic resources in a campaign that is intended to support a larger strategic plan that may have nothing to do with the Arctic.

Russia will be, if it is not already, one of the world's leading Arctic powers. It possesses at least half of the Arctic in terms of area, coastline and population. Russia is making plans and entering into business arrangements with major energy companies to exploit the Arctic's vast energy resources. However, as global climate change transforms the Arctic environment, Russia sees a substantially expanded potential for the Northern Sea Route (NSR) that stretches along the length of its northern, Arctic coast. Russian commercial shipping already uses the NSR, but the NSR's shipping season is still relatively short – only four to five months per year. This is expected to increase significantly in the coming years due to climate change, and it is possible that by the 2050 timeframe, if not sooner, the NSR could be a year-round transit route that plays a major role in Russia's economic development plans for the 21st century. It takes a merchant ship forty percent less time to sail from Murmansk to the Bering Sea via the Northern Sea Route than it does to go by way of the Suez Canal. Using the NSR would also cut the distance between Rotterdam and Shanghai by twenty-two percent. (By comparison, using the Northwest Passage in Canada's Arctic region would reduce that Rotterdam-Shanghai distance by only fifteen percent.[39]) Map 2 (below) depicts the larger Arctic region, but clearly shows the Northern Sea Route and that Russia would likely be the dominant state actor of the region.

[39] The Northwest Passage, much of which is still uncharted, is also less accessible than the Northern Sea Route because of the ice floes around Canada's many Arctic islands; as such, the Northwest Passage currently has much less commercial shipping traffic and infrastructure than Russia's Northern Sea Route.



Map 2: The Arctic Region

(Source: CIA World Factbook)

As the NSR's shipping season increases beyond the current four to five months per year, there will doubtless be more shipping infrastructure constructed along Russia' Arctic coast - from piers and port facilities, to oil and coal terminals, to railheads that transport the coal and oil from Russia's interior to its developed Arctic ports. Some of this infrastructure may not necessarily be developed on the Russian mainland. Temporary or re-locatable facilities (such as weather stations, search and rescue facilities, and pilot stations) also could be built on major ice floes in the Arctic. Asia's major exporters (Japan, China and Korea) are reportedly investing in ice-capable ships to take advantage of the NSR, which also increases the incentive for Russia to invest in enhancements to its Arctic infrastructure. Thus, it is possible to view the future Arctic shipping lanes as a 21st century equivalent of the historic "Silk Road" that crossed the Eurasian land mass centuries ago. Just as no one kingdom or power could dominate the entire Silk Road, no one actor will likely dominate all of the Arctic's future shipping lanes. Some will be in territorial waters, others in international seas. Yet, it will likely require the efforts of all Arctic actors to ensure the Arctic shipping lanes remain open and uncontested.

The Scenario

At some point in the 21st century, Russia could come into conflict with a major state or coalition of states, and the United States may not necessarily be a participant. The immediate cause of the conflict could range from ethnic disputes in former Soviet republics to the resurgence of age-old animosities with certain European actors. Regardless, any future adversary of Russia

will, as part of that larger conflict, not only seek to target Russia's Arctic energy facilities (sea- and land-based) but will also attempt to interdict Russia's Arctic sea lines of communication (SLOCs) that increasingly link Asian eastern Russia with European western Russia, or are used to export Russian energy derived from the Arctic to the world energy market.

Given the vulnerabilities of its Arctic energy assets and SLOCs, Russia would naturally attempt to deploy increasing numbers of its own A2/AD systems to defend them. In particular, it would likely focus on advanced long-range surface-to-air missiles, coastal defense anti-ship cruise missiles, submarines (both nuclear- and conventional-powered), a range of surface naval forces (from coastal missiles boats – more able to operate in Arctic waters due to global climate change – to major surface combatants), complemented by short- and long-range land-based air and ballistic missile power. In addition, Russia would be wise to invest in ballistic missiles defenses for its fixed Arctic energy facilities, as they would likely be prime targets for an adversary's conventional ballistic missiles.

The Campaigns

This scenario envisions two major, but inter-related campaigns by an adversary that would be conducted in Russia's Arctic region. The first would be a campaign directed at Russia's energy infrastructure in the region. The objective of the second campaign would be to interdict Russia's sea lines of communication (SLOCs) in the Arctic Ocean.

The ***anti-energy infrastructure campaign*** would consist of a wide range of operations. An important preliminary operation to the anti-energy infrastructure campaign would be a **C4ISR/cyber operation** to determine the extent and location of Russia's energy assets in the Arctic, with an emphasis on determining which would result in the greatest disruption to Russian energy resources by their destruction or major disruption. These C4ISR/cyber operations would have to be conducted for the duration of the campaign and its aftermath to monitor Russia's ability to repair and/or replace its damaged or destroyed energy facilities.

Operations intended to physically damage and/or destroy major elements of Russia's Arctic energy assets could take a number of forms. Such operations would include **attacks by special operations forces and/or commandos**, as well as **physically-destructive cyber attacks**. (Moreover, since the Arctic campaigns would likely be facets of a larger conflict with Russia, where there are no longer any "front lines," special operations and cyber attacks would also likely be conducted against homeland targets.) Other strikes against this infrastructure could be conducted by sea-based systems and land-based systems (from ballistic missiles and land-attack cruise missiles, to armed drones and long-range land-based manned aircraft or unmanned aerial reconnaissance/strike vehicles).

The Arctic environment also presents opportunities for the innovative employment of forces, such as the use of ice floes as Forward Operating Bases (FOBs) or in international waters for the re-fueling and re-arming of, for example, attack helicopters or armed drones against Russian energy facilities. The FOBs could also be used by special operations forces that are conducting ISR and/or attack missions. These FOBs could, in turn, be sustained by submarines, specially-configured supply ships, or supplies delivered by parachute from manned or unmanned aircraft.

The ***SLOC interdiction campaign*** would resemble a traditional sea-denial campaign, but with certain characteristics unique to the Arctic operating environment. The enormous length of Russia's Arctic coast and its NSR would place a major burden on the adversary's **C4ISR/cyber network** to adequately detect, track and target Russia's commercial shipping traffic in the region. The adversary's submarines and/or aircraft would likely be employed to lay **mines** in key shipping channels or the entrances to major harbors. Sea-based and/or land-based aircraft and armed drones, possessing sufficient range and endurance, would also conduct ISR/attack missions against Russian shipping.

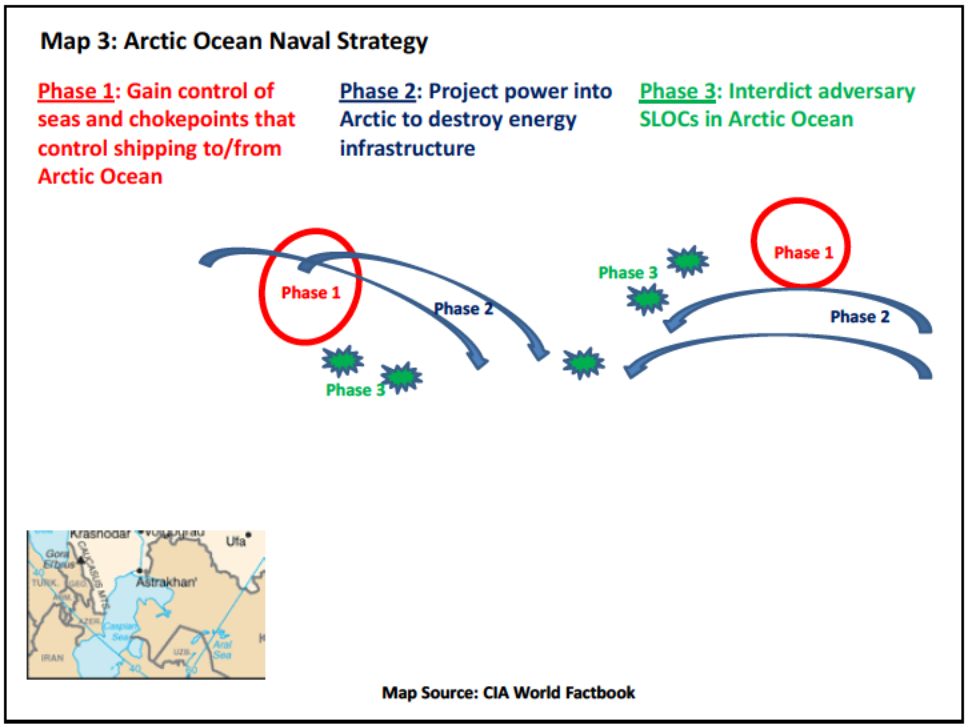
Attack submarines would also be employed to detect and track Russian shipping, with attacks being executed by either torpedoes or anti-ship cruise missiles. Currently, nuclear-powered submarines (SSNs), with hulls and superstructures strengthened for under-ice operations, are best suited employment in the Arctic. If the United States were the potentially adversary in this scenario, U.S. Navy SSNs based, for example, at the current submarine bases in Connecticut and Washington would have relatively short transit times to the Arctic Ocean – they could be on-station in Arctic patrol areas in a matter of days due to their high-submerged transit speeds, and their endurance would enable them to remain on deployment for many weeks. The only limiting factors are the number of weapons they can carry to attack shipping and the amount of food onboard to sustain the crew. Therefore, since SSNs are already extraordinarily expensive platforms, the naval architects of today may want to consider the cost trade-offs of expanding the weapons and provisions loadouts of future generations of new SSNs for a range of conflict scenarios.

With the substantial diminishment of ice in the Arctic due to climate change, modern conventionally-powered attack submarines (particularly ones equipped with systems such as Air Independent Propulsion [AIP]) will be able to operate more effectively in this region than they can at present. Thus, mid-size state actors that cannot afford large, expensive nuclear-powered submarines today, will be able to potentially threaten Russian Arctic SLOCs in the future with affordable forces of conventionally-powered submarines.

As in the anti-energy campaign, special operations forces and physically-destructive cyber attacks could also be employed in the anti-SLOC campaign. SOF could be used to destroy key harbor facilities or even board and capture key Russian ships. Physically-destructive cyber attacks could be employed to disrupt loading operations of commercial ships in a port, or to disable the propulsion plants of the ships while at sea.

How the Campaigns Will Play Out

The ***anti-energy infrastructure campaign and anti-SLOC campaign*** would unfold in three phases (see Map 3 below), as did the campaign waged against Chinese energy infrastructure in the South China Sea.



Map 3: Arctic Ocean Naval Strategy

(Map Source: CIA World Factbook)

While Russia's Arctic coast is very long, and its Arctic territorial waters vast, they are bounded at each end by chokepoints. On the East, is the Barents Seas; to the West is the Bering Sea, which includes the relatively narrow Bering Strait. The objective of Phase 1 of an Arctic Ocean naval strategy would be to gain control of those chokepoints to prevent any commercial and naval shipping from entering or departing Russia's Arctic waters. The narrow Bering Strait could be closed by a combination of minefields, land-based anti-ship cruise missiles and ISR/strike drones, and submarines and stealthy surface combatants that patrol the waters off the southern entrance to the strait, most likely outside the range of Russian A2/AD systems.

The Barents Sea would present a greater challenge to control during Phase 1. However, again, a combination of minefields, submarines and land-based strike systems would be in the forefront of this Phase, supported by surface forces specially designed for sustained operations in the Arctic environment.

Phase 2, which could be conducted simultaneously with Phase 1, would consist of long-range, precision attacks against Russia's Arctic energy facilities, most of which would originate from outside the Barents Sea and Bering Sea chokepoints that were blocked during Phase 1. They could be conducted by either sea-based platforms (again, strengthened for sustained operations in Arctic waters), or by a range of land-based systems. They would likely be supported by long-range, unmanned ISR assets that would be used to evaluate the success of the strikes and monitor Russian attempts to replace and/or repair damaged facilities.

The long-range attacks of Phase 2 could be complemented by attacks from, for example, nuclear-powered submarines operating in Russia's Arctic waters, most likely by land-attack cruise missiles. However, submarine torpedoes could also be employed against some of Russia's fixed, offshore facilities as well. Special operations forces could be based on ice-flow FOBs to either provide ISR support, or conduct their own attacks.

Russia's adversary could, in an effort limit the physical damage to Russian facilities, if it were so inclined, conduct siege-like operations against some of Russia's more remote or isolated Arctic energy facilities. Instead of destroying them outright, the adversary could select certain facilities for a type of Arctic-siege, where the lines of communications that sustain these facilities are cut in the attempt to either deny their use to Russia or get them to surrender and turn over physical control of the facility to, say, the adversary's special operations forces.

Phase 3, the ***anti-SLOC campaign*** would be somewhat reminiscent of World War II's convoy battles in northern, Arctic waters. The key variable is whether Russia's adversary could deploy enough naval power (specifically submarines) into the Arctic to overwhelm any Russian naval power that would be defending its commercial shipping. Russia could have the ability to shift its naval forces rather rapidly between its European West and Asian East because of the year-round, relatively near-ice-free conditions along its the Northern Sea Route, but Phase 1's objective of gaining control of the Barents and Bering Sea chokepoints would prevent Russia from deploying any additional naval power into the Arctic from its non-Arctic waters. Any Russian naval reinforcements would first have to break through the chokepoints before it could help defend Russian Arctic SLOCs.

Sustained C4ISR/cyber support would be needed for the duration of the three Phases. During times of tension or crisis, Russian C4ISR would be on the alert for the deployment of an adversary's forces into the Arctic or to the vicinity of the Barents and Bering Seas. Russia would then probably initiate measures to augment its A2/AD systems that defend its Arctic assets.

Once the conflict started, the adversary would likely conduct strike operations in either short bursts against specific targets, or in a massive bombardment intended to destroy the majority of Russia's Arctic assets in as short a time as possible.

Nevertheless, this Arctic strike campaign would be waged over a much larger geographic area (virtually the length of Russia's Arctic coast), under much harsher environmental conditions than found in the Western Pacific and Indian Ocean. Thus, this campaign should be expected to take far longer than its South China Sea counterpart.

The key question for the adversary that is confronting Russia in the Arctic in both of these campaigns is whether the damage inflicted on its energy infrastructure and commercial shipping is sufficient to compel Russia's surrender, or push Russia into considering an escalation of the conflict to where nuclear weapons become an option.

Force Requirements

The air and naval forces that would be used to attack Russia's Arctic SLOCs and energy infrastructure would require many of the same characteristics and features found in the force that would attack China's energy facilities in the South China Sea. These include substantial endurance, large payloads of long-range precision strike weapons, and minimally-manned and/or autonomous platforms.

However, while the Arctic will become a more likely area for future combat due to climate change, it will not be an ice-free region. The still-harsh environment of the Arctic circa 2050 will place more strenuous operating demands on a force than the environments of the Indian Ocean or Western Pacific.

Despite the impact of global climate change on the Arctic, with the subsequent significant decrease in Arctic ice coverage, the Arctic will still be an inhospitable region. Major parts of the Arctic Ocean will still be covered in ice or semi-frozen. For much of the winter, there will be light sunlight, with temperatures that will continue to make it a hostile environment for man and machine. Thus, unmanned vehicles (both aerial and maritime) and/or robotic systems that can be designed to operate in the Arctic could have an advantage over manned ones due to the extra logistical requirements of supporting people in such an environment

The Arctic Ocean will be still one of frozen or semi-frozen seas, and navigating them will not be simply a matter of breaking through the ice. Navigating these waters will still require selecting a route through hidden ice currents to avoid the ice floes that can severely damage the hulls of all but the toughest ships. Thus, while a naval force of *Many, Cheaper, and Unmanned* ships could deploy to this region, they would have to be built to a much tougher design than the *Many, Cheaper, and Unmanned* fleet intended for the South China Sea anti-access scenario. The Arctic, then, may well be an ocean more suited for high-endurance submarines, than surface ships or semi-submersibles.

Moreover, the seamanship required to safely operate in these waters is a skill that cannot be acquired quickly. Whether such seamanship "skills" can be incorporated into a *Many, Cheaper, and Unmanned* fleet for the Arctic will be a major technological challenge.

The costs of designing and building a large naval force optimized for sustained Arctic operations could be prohibitive, and even a major naval power may only decide to build a small number of units capable of operating in those waters. This could likely compel an adversary to consider deploying long-range conventional land-based strike systems that could hold Russia's Arctic assets at risk, such a ballistic missiles, land-attack cruise missiles, and/or unmanned aerial combat vehicles or attack drones.

The Commodity Access/Denial Competition

As the likely competition for the critical resources necessary to maintain the global economy increases in the coming years, it is increasingly likely that the range of state actors not in possession of the critical resources ("non-possessors") will attempt to use international law and

new norms of behavior between states to assert that the "possessor" state must grant access to these critical resources in the name of the greater global economic good. In an increasingly inter-connected, globalized world with global citizens, competition for resources could result in global claims on resources – by states (of various ilk) or by non-state actors; in other words, a state's sovereign rights to control the resources within its borders may be challenged because a global citizenry will demand access to these resources for the global good, or armed conflict may ensue.

Such a scenario clearly threatens traditional, post-Westphalian notions of state sovereignty. Yet, there are analogous examples today of this new phenomenon, although they are currently limited to humanitarian-related issues. In 2011, as the uprising against Libyan dictator, Muammar Gaddafi, raged and seemed to be turning in favor of the regime, there was international outcry by some to intervene in the conflict on behalf of the rebels. This is an example of what has become known as the right of humanitarian intervention, where the global community intervenes in what has traditionally been considered a sovereign state's affairs to stop the oppression of the state's peoples. Gaddafi's regime fell, with the rebels receiving some support from regional actors, while ongoing civil conflict/unrest in Syria has led to renewed calls for a humanitarian intervention in that country. It remains to be seen if such a humanitarian intervention takes place in Syria, but humanitarian intervention was one of the grounds used to justify NATO's involvement in Kosovo in 1999.

In the coming decades, given trends in energy and non-energy resources described in previous chapters, it is not unreasonable to assume that the type of emphasis placed on humanitarian intervention today in the name of the greater global good will also be placed on "resource intervention," also in the name of the greater global good. Humanitarian intervention is based on the notion that a sovereign state no longer has "the right" to repress or harm large segments of its population and that the global community has the responsibility to compel that state (with military force if necessary) to treat its citizens humanely. Resource intervention would likely be based on a similar premise: that a sovereign state no longer has exclusive rights over any critical resources that may reside within it's internationally recognized borders. If that state denied the global community its "rightful" access to those resources in the name of, for example, sustaining the global economy or preventing a shortage that could adversely impact living standards, then the global community would be justified in pressuring that state into providing such access (through the threat of military force if that is what is required).

As the globalized economy demands greater and greater "specialized" resources found only in certain countries, the "global right" to these resources will increasingly be employed to gain access to these resources. Unless such access is granted, it is not outside the realm of possibility that an armed coalition could be formed—perhaps comprised of state and non-state actors—to compel the "possessor" state to share its critical resources with the global "community" for the good of all.

Before an explicit military coalition would be fashioned, it is likely that other forms of pressure would be employed against the "possessor" state to share its resources. Such pressure could come in the form of economic warfare, cyber attacks, a vigorous social media "propaganda"

campaign, or even special operations "actions" by third-parties' forces to apply selectively destructive pressure on the "possessor" state. These actions would be significant, strategic level actions intended to achieve specific policy objectives. In fact, the non-military forms of the competition could potentially be much less costly than developing military forces, opening the door for broader array of actors to play a role in compelling the "possessor" state.

In addition, smaller states that need access to a larger state's reservoir of critical resources could form an alliance that exerts pressure on the "possessor" state that, in relative terms, is much greater than the sum of their traditional military parts, particularly if they take advantage of the emerging *Many, Cheaper, Unmanned* paradigm of warfare. They could develop forces that rival or exceed the capability of the "possessor" state they wish to coerce. The smaller states could form alliances of non-possessor states that would seek to exert "pressure" on the larger, possessor state to be more "sharing" with its resources. For example, it is frequently reported that the smaller states of Europe have no recourse but to sometimes accede to the "blackmail" of the Russian state that provides them with much needed natural gas. While military power would not be a viable option to counter that Russian "blackmail" the employment of new, strategic-level forms of influence (e.g. an intense strategic communications campaign to shift public opinion or a plausibly deniable cyber campaign to disrupt critical infrastructure) could very well be employed against a Russia that may not be equipped to counter them.

To resist such pressure, the "possessor" state would actively engage in a series of competitions to counter the forms of pressure cited above. Thus, the "possessor" state would engage in international legal actions to counter the arguments of "non-possessor" states.

In turn, the "non-possessors" would escalate their actions in the competition in order to keep pace. The nature or intensity of this competition would likely depend on how important the critical resource is to the global economy. The more critical the resource, the greater the stakes, and the more likely the competition will escalate.

The Scenario

This scenario envisions a conflict over access to "specialized" resources. As the world economy demands increasing amounts of "specialized" resources found only in certain countries (in this case, Malaysia), the "global right" to these resources will increasingly be asserted to gain and/or justify access to them. Unless such access is granted, it is possible that an armed coalition could be formed, perhaps comprised of state and non-state actors, to compel the "possessor" state to share its critical resources with the global "community" for the good of all.

For example, Malaysia currently is developing a rare earth mineral mine and is likely to soon become a global leader in rare earth mineral production. If Malaysia attempted to deny these resources to its Southeast Asia neighbors, a coalition of Southeast Asian states might form to force Malaysia to change its export policy.

The Campaign

The coalition campaign against Malaysia would not rest solely on explicit military kinetic operations. Instead, other forms of pressure would be employed against Malaysia (the "possessor" state) to share its resources. A key component of a non-military approach would be a strategic communications effort to shape the international opinion towards Malaysia. A vigorous social media "propaganda" campaign would be a robust and, potentially, highly effective approach. The coalition could also rely on more direct forms of pressure, including economic warfare, cyber attacks, or even special operations "actions" by third-parties' forces to apply selectively destructive pressure on Malaysia. These actions would be significant, strategic level actions intended to achieve specific policy objectives. In fact, the non-military forms of the competition could potentially be much less costly than developing military forces, opening the door for broader array of actors to play a role in compelling Malaysia.

How the Campaign Would Play Out

The Southeast Asian coalition would likely begin with a sustained, multi-pronged social media operation intended to both pressure Malaysia and to garner broader support. The Internet would likely be ground-zero for such a media operation. The Southeast Asian coalition would seek to shape and influence regional and international opinion, with the individual states operating fairly autonomously, only minimal coordination would be needed to establish the overall message and tone.

Unless Malaysia immediately acceded to their adversary's demands, the two actors would likely enter into an escalating series of actions to increase the coercive pressure on each other. The nature or intensity of this competition would likely depend on how important the critical resource is to the global economy. The more critical the resource, the greater the stakes, and the more likely the competition will escalate.

To resist such pressure, Malaysia might attempt to launch its own strategic communications campaign. However, facing multiple states operating concurrently in that environment, Malaysia might seek to shift the conflict into another arena. One potential action would be to engage in international legal actions to counter the arguments of the Southeast Asian coalition.

In turn, the Southeast Asian coalition would escalate their actions in the competition to maintain the pressure. At this point, the coalition could turn to plausibly deniable cyber attacks, especially those that disrupt activities rather than damage or destroy. This would increase coercive pressure, but avoid undermining international sympathy for the coalition's cause. More overt operations, such as economic warfare in the form of boycotts or embargoes, likely would follow. At this point, the coalition would have decided that the potential for losing some international support was less important than increasing direct pressure on Malaysia.

Force Requirements

The Southeast Asian coalition would exert pressure on Malaysia that, in relative terms, is much greater than the sum of their traditional military parts, particularly if they take advantage of the emerging *Many, Cheaper, Unmanned* paradigm of warfare. They could develop forces that rival or exceed the capability of Malaysia. However, the force requirements are not necessarily tied to traditional, expensive military platforms. Indeed, investing in significant military capability could undermine the strategic communications campaign by reducing international sympathy. Each state would only need to invest a modicum of resources to buttress their existing media capabilities; launching a Twitter campaign costs next to nothing. Consequently, the full panoply of Southeast Asian states could join the coalition.

The Physically-Destructive Cyber Competition

Perhaps more than any other of the military and/or technological competitions of the future, the physically-destructive cyber competition is the one has the potential to "level the playing field" between large states and smaller ones, and between various state actors and non-state actors. Moreover, as the capability to inflict such physical cyber destruction on an adversary increases, small states and non-state actors will likely see the deterrent advantage this competition gives them.

A basic premise of the future security environment posited in this paper is that there will be more non-state actors on the world stage in the coming decades, and state actors will increasingly have interests that clash with the political goals of non-state actors. Such clashes could originate for a wide range of reasons – from traditional disputes over borders and territory (particularly those territories where critical resources are located), to political disputes over the treatment of ethnic populations. Thus, there will be many more opportunities and incentives for actors (state or non-state) to conduct physically-destructive cyber attacks as part of some larger campaign or conflict, regardless of its origin or source. Future cyber mercenaries will sell their services to the highest bidder; all the combatants need to compete are the financial resources to pay for the "brain power" (domestic or foreign) to plan and conduct cyber attacks. Non-state actors (perhaps funded by nation-states that serve as "sponsors") could provide sanctuary for these mercenary cyber-warriors to plan or conduct their attacks.

Moreover, such state versus non-state actor conflicts could occur between a state and a non-state actor operating within the recognized borders of another state actor (i.e., Israel and the PLO), or between a non-state actor and the state whose territory it resides in (examples include Hezbollah and the government of Lebanon today, or the PLO and the government of Jordan in the early 1970s).

Thus, the competition likely at the center of such a conflict would be cyber-based, but not the commonly appreciated cyber competition of today where "hackers" (working for governments, non-state actors, or on their own) wreak havoc on the Internet (though cyber actions such as

this will likely still be a concern in the future decades). Instead, this competition would be about the ability of actors (state, non-state, terrorist groups, or individuals) to use cyber space to wreak physical destruction on the key military, civilian and/or economic infrastructure of an adversary. The resources to develop such a capability are very intelligent "cyber-savvy" programmers that have the talent to engineer such attacks, and sufficient funds to pay for their services.

Using a contemporary example, this conflict takes the reported "Stuxnet" cyber attacks against Iran's nuclear facilities to a much greater level. In this competition, rivals would have the ability to cause a piece of equipment to self-destruct or destroy another piece of equipment by "ordering" it do so via the Internet. In an increasingly "hyper-connected" world, major facilities and equipment will need to be networked to function efficiently and effectively. Yet, such hyper-connectivity will also create a web of vulnerabilities – the very "inter-connectedness" that leads to increased efficiency and effectiveness also exposes those that are inter-connected to new forms of cyber "attacks" and "sabotage" by adversaries.

Today, as evidenced by the cyber attacks on Iranian nuclear facilities, there is a credible threat against major power generating plants, industrial facilities, and the like. For example, a cyber attack against the physical power generating plant (either the primary or backup) of a major military installation could cause a turbine generator to spin out of control, destroying itself, thereby "blacking out" that military base. Such an attack could be launched by third parties to provide the real sponsor with plausible deniability. In addition, such an attack could be conducted at a time when tensions between the adversaries are low such that the attack serves as a warning to the state actor that it is vulnerable at any time.

In the near future, such physically destructive cyber actions will be a credible threat that can be employed against vehicles, aircraft, ships, airports and rail networks - anything that is connected to the Internet. Imagine a very large container ship or tanker entering a major port having its controls taken over by a "hacker" on the other side of the world who directs the container ship to crash into other ships in the channel, effectively blocking it for an unspecified amount of time.

While such a competition would pose a substantial danger to the civilian infrastructure of a developed state (which could be an emerging form of cyber deterrence akin to the Cold War notion of mutually assured destruction against a rival's major city), the military implications of this competition also need to be considered.

The cyber warriors of a non-state actor or of a small state could "hack" into the control systems of a tank or jet aircraft, forcing them to "burn out" their engines (which cannot be easily, quickly or cheaply replaced) or detonating a missile in the magazine of a warship or a combat aircraft. Such an attack could be launched with the intent only to disable the enemy unit, and assumes that the tank or aircraft was not totally destroyed when its control systems were "hacked." Yet, the actual destruction of the weapon system itself could also be a goal of the cyber warrior, which likely could result in a competition between the cyber warriors to see who can become the first "cyber ace." Today a fighter pilot is considered an "ace" when he/she

shoots down five enemy aircraft. In the not-too-distant future, will five "kills" be the number needed to become a "cyber ace?" (One can only speculate what such a capability will have on a military's traditional "warrior culture," but one can imagine a future cyber warrior having the silhouettes of his "kills" stenciled on the side of his/her computer.)

The range of possible destructive cyber attacks is enormous. A small state or non-state actor could re-program the precision strike targeting systems of the large state to target the large state's forces and/or installations. A major warship, sitting offshore the small state or non-state actor's coast, could suddenly find that its propulsion plant had suffered a series of casualties that leaves the major warship lying dead in the water, without power for its weapons systems, at the mercy of its adversaries' forces.

The possibility of actual armed conflict still exists in the future, but on the first day of an actual armed conflict the large state could also find its "home front" on the "front lines," as adversaries wreak cyber-inspired destruction throughout its economy and society (e.g. disruptions to radio or television broadcasting, social services, or social media). This raises the potentially disturbing prospect of a "cyber 5th column" pre-planted in the targeted nation-state. Instead of adversary-sponsored saboteurs blowing up bridges behind enemy lines, "cyber saboteurs" will do the same thing, but future cyber saboteurs will be very difficult to find and apprehend, even if they are operating from within the borders of the attacked state.

This type of physically destructive cyber competition will almost certainly compel states either to take themselves "off the net" altogether to decrease the risk of physical cyber attack, but this will come at the cost of effectiveness and efficiency, which also plays into the hands of the smaller adversary. Or, states that seek to engage actively in this competition will be forced to continuously monitor and upgrade their "netted" systems, a costly process that could drain resources away from other military programs. More realistically, it will be a combination of both.

The Scenario

A potential scenario for this type of conflict could be between Turkey and Kurds living within the borders of Iraq and Iran, "next door" to Turkey. Kurds, a distinct ethnic group of some 30 million people in the Middle East (mostly in Iran, Iraq, Syria and Turkey), have a nationalist movement that strives to establish and independent Kurdish state. Part of this movement has turned to violence to achieve its objectives and to fight against discrimination and violence against Kurds. In particular, Kurds have conducted what amounts to terrorist operations in Turkey for years. In the future, unable to take on the formidable Turkish military, the Kurds could turn to destructive cyber attacks to level the playing field. The Kurds' objective with the destructive cyber attacks would be to deliver punishment to Turkey to coerce the Turkish government to accede to the Kurdish demands.

The Campaign

The Kurds would likely launch physically destructive cyber attacks against both the civilian and military sectors in Turkey. In the near future, physically destructive cyber actions will be a credible threat that can be employed against vehicles, aircraft, ships, airports and rail networks - anything that is connected to the Internet. Likewise, the infrastructure and equipment supporting the military sector would be vulnerable.

Disabling or destroying elements of the civilian infrastructure could have a significant impact on economic production. Industrial facilities, such as major power generating plants, typically have extensive connections to the Internet and are vulnerable. A cyber attack against the power generating plant (either the primary or backup) could cause a turbine generator to spin out of control, destroying itself, thereby causing a widespread "black out" with significant consequences to the local economy. But cyber attacks could also target individual pieces of equipment. Imagine a very large container ship or tanker entering a major port or waterway (such as the Bosporus) having its controls taken over by a "hacker" on the other side of the world who directs the container ship to crash into other ships in the channel, effectively blocking it for an unspecified amount of time.

A campaign against the Turkish military sector also would target infrastructure, but would likely include direct cyber attacks on deployed forces if possible. Destructive cyber attacks could lead to destruction either indirectly or directly. An indirect approach would severely degrade or incapacitate a piece of equipment or platform, rendering it highly vulnerable to follow-on attack by conventional military forces. An example would be disabling the fire-control radar/capability of a surface-to-air missile battery. The direct approach could either disable or destroy the equipment. For example, Kurdish cyber warriors could "hack" into the control systems of a Turkish tank or jet aircraft, forcing them to "burn out" their engines (which cannot be easily, quickly or cheaply replaced). More damaging would be detonating a missile in the magazine of a Turkish warship or a combat aircraft. Interestingly, such an attack could result in a competition between the cyber warriors to see who can become the first "cyber ace."

How the Campaign Would Play Out

The Kurds would have many options in launching their campaign. For maximum effect, they could opt for a full-blown attack against both civilian and military sectors to cause as much damage as fast as possible before Turkey could react sufficiently. However, that also has the potential of massive counter-reaction from Turkey as well as the potential for the Kurds expending their entire "arsenal" of cyber weapons in one blow. If that blow fails to achieve its objectives, then the Kurds will have failed.

Instead, the Kurds would likely adopt a more traditional coercive diplomacy strategy of inflicting an escalating series of attacks to exert an increasing amount of pressure on the Turkish government. The Kurds might initially seek to avoid direct responsibility for cyber attacks, conducting the attacks to demonstrate Turkey's vulnerability. Eventually, the Kurds would

need to tie themselves to the attacks as a way to achieve coercive pressure. The escalating nature of the attacks would likely serve as a warning to the Turkish government that failure to accede to Kurdish demands would lead be progressively more painful action against Turkey. At its peak, the Kurds would seek to put Turkey's "home front" on the "front lines," as cyber-inspired destruction wreaks havoc throughout the economy and society (e.g. disruptions to radio or television broadcasting, social services, or social media).

Most likely, the Kurds would start with a dual-sector approach, causing disruptions in both the civilian and military sectors. Oil pipelines could suffer successive pump station failures, shutting down operations. A major warship could suddenly find that its propulsion plant had suffered a series of casualties that leaves it lying dead in the water.

Turkey would likely face difficult decisions on how to react. Direct kinetic attacks against Kurdish secessionist organizations tied to terrorist acts (such as the PKK) in neighboring states would be an option, but Turkish military capability might be degraded by the cyber attacks. Direct responses against the cyber warriors would be problematic. Identifying their geographic location would be challenging since the cyber warriors might be located far from the Middle East to preclude easy physical retaliation. Tactically, Turkey would need to mitigate the vulnerability to additional cyber attacks. Turkey might be compelled to take itself "off the net" altogether to decrease the risk of physical cyber attack, but this would come at the cost of effectiveness and efficiency, which also would play into the hands of the Kurds. Or, Turkey would be forced to continuously monitor and upgrade their "netted" systems, a costly process that could drain resources away from other military programs. More realistically, it could be a combination of both.

The extent and scope of the Kurdish escalation almost certainly would be tied to the Turkish reaction. If Turkey relied on military force to retaliate, the Kurds could inflict damage to deployed Turkish forces. Even more ominous, the Kurdish cyber warriors could re-program Turkey's precision strike targeting systems to target their own forces and/or installations. Another possibility is a cyber version of Israel's pre-emptive attack on Arab air forces during the 1967 "Six Day War." Yet, instead of destroying the enemy air forces on the ground in a risky pre-emptive air attack, physical cyber destruction could be directed at the enemy's air forces while they are still on the ground, without risking a single pilot or plane.

Force Requirements

An actor attempting to conduct a destructive cyber campaign probably would pursue the *Few, Expensive and Manned* paradigm for expending resources. To conduct the sophisticated cyber attacks, an actor will likely need highly-qualified technical experts and highly specialized equipment. The ability to conduct such a campaign would hinge upon whether the actor can develop the very intelligent "cyber-savvy" programmers that have the talent to engineer such attacks, and sufficient funds to pay for their services. Indeed, an actor may not choose to invest in "home-grown" talent, but instead seek the necessary expertise elsewhere. Future cyber mercenaries will sell their services to the highest bidder; all the combatants need to compete

are the financial resources to pay for the "brain power" (domestic or foreign) to plan and conduct cyber attacks. Their geographic location will not be important; they need access to the internet not close proximity to their target.

There also is the potentially disturbing prospect of a "cyber 5th column" pre-planted in the targeted nation-state. Instead of adversary-sponsored saboteurs blowing up bridges behind enemy lines, "cyber saboteurs" will do the same thing, but future cyber saboteurs will be very difficult to find and apprehend, even more so if they are mercenaries operating on behalf of a non-state actor.

The *Many, Cheap and Unmanned* paradigm, though, should not be ruled out. Currently, sophisticated cyber attacks require highly-trained personnel, which inherently means that there are relatively few people with the necessary skill set. However, in the future, the expertise and knowledge and technology needed to conduct these types of attacks could well be more widely available. In this case, the *Many, Cheap and Unmanned* paradigm might emerge as a viable option. A bevy of programmers with limited skills, but who require little investment of resources, could leverage semi-automated or foreign off-the-shelf technology to develop a credible destructive cyber attack capability.

The "Special Operators" Competition

This competition can be conducted by virtually every actor in the future security environment, as it foresees the widespread adoption of special operations-like, irregular forces by these actors. There could be a wide range of scenarios in which such a competition and/or conflict would play out. They include, but are certainly not limited to, a *dysfunctional state* attempting to squash a non-state actor within its borders that is advocating for its own homeland, to a nation-state engaging with a non-state actor in a prolonged conflict based on extreme religious and/or ideological philosophies. Or, the scenario could involve a violent conflict between two non-state actors, vying for dominant influence in a region of the world that nation-states consider "ungoverned."

This paper envisions that today's definition of special operations forces (SOF) will be greatly expanded in the future. Indeed, a number of future actors may follow the lead of Iran, whose military forces today are largely dominated by the "SOF-like" forces of the regime's Revolutionary Guard. Today, the term SOF is rather narrowly applied to the commando-style, elite units of modern military forces operating under the auspices of a state. Today's "SOF" also includes elements of the intelligence services that specialize in SOF-like operations in the field, and it is also an arena of conflict in which private contractors are operating at what appears to be ever increasing numbers. In the future security environment of 2035-2050, with its increased number of state and non-state actors, the definition of "special operators" will broaden to include the irregular forces employed by an actor (state or non-state) to conduct non-traditional military-type operations. Thus, while future "special operators" in this competition will still include the SOF of modern militaries (such as the Navy SEALs or Army

Delta of the United States), it will also include the elite fighting units of the military wing of non-state actors (i.e., Hezbollah and Hamas) and even the suicide bombers of ideologically or religiously motivated groups.

How receptive will the future's "special operators" be to the wide range of new technologies that will be available to them? Most likely they will warmly embrace any technology that increases the chances of mission success and operational effectiveness, with examples ranging from the armed drones conducting attacks on terrorist targets in Afghanistan, Pakistan and Yemen, to the increasingly sophisticated IEDs being employed by some of those same terrorists against U.S. troops in Afghanistan.

The Scenario

Perhaps the most illustrative scenario of the scope and extent of potential conflict would be a violent conflict between two non-state actors, vying for dominant influence in a region of the world that nation-states consider "ungoverned." The fighting by non-state actors in the eastern Democratic Republic of Congo (DRC) would be a good representative example. Fighting in this region has been ongoing for years, sparked by ethnic tensions and supported by money gained from extraction of natural resources; it is likely to continue for years to come. Groups and militia comprised of ethnic Hutus, driven from neighboring Rwanda after the genocide there in 1994, are in conflict with ethnic Tutsi groups and militias. The two ethnic groups are primarily fighting for control over eastern DRC. The Hutus want to retain control over a base with which to strike at the Tutsi-controlled Rwandan government, while Tutsi wants to eradicate the Hutu militias and or drive them away from Rwandan territory. Both sides have killed many, mostly civilians, but have been unable to deliver a decisive blow to the other. In the future, seeking to generate more military capability, but realizing that traditional military forces have difficulty operating in the challenging mountainous terrain of eastern DRC, both groups could develop SOF-like operators to supplant their militias.

The Campaign

Both the Hutu and the Tutsi forces would execute SOF-like operations against the others' military and commercial assets to degrade their respective capabilities to conduct military activities and to generate revenue. Counterforce attacks would likely target command units and logistics networks to degrade overall capabilities; direct attacks against field military forces (even if low-value militia units) would be much less likely. Countervalue attacks would likely target extraction and transportation infrastructure and equipment, e.g., the mines where minerals are extracted and the trucks that carry the few minerals to processing plants and/or export facilities. The goal would be not to destroy the infrastructure entirely, but merely to reduce its throughput; if successful in driving out its adversary, each side would seek to maintain resource extraction at the highest possible level.

How the Campaign Would Play Out

The campaigns would likely be prolonged, but relatively low-intensity and somewhat erratic in execution, consistent with the informal operational structure and practice of these non-state actors. Neither side is likely to develop a large SOF-like capability so that only a limited quantity of operations could be ongoing at any time. Both sides likely would use their SOF-like capability in a rather haphazard manner as neither side has demonstrated an ability to develop and execute strategic military operations. Instead of concerted efforts against counterforce or countervalue targets, each side likely would attempt a mixture. Some attacks against natural resource infrastructure would occur to destroy equipment as well as to intimidate workers. Whereas militias attacks against these targets often result in damage not nearly commensurate with the ammunition expenditure, SOF-like forces will deliver much more effective attacks. The scope and scale of the damage from their attacks would likely be significantly more than previous operations. Other attacks against military capability would occur as well with some in conjunction with militias. In other words, the SOF-like capability would be a crude force multiplier for both sides, striking an opponent's C4ISR as a prelude to a militia-based attack. While the SOF-like capability of each side would enhance overall military capability, their impact at the strategic level is more questionable. Each side would need to develop more coordinated, coherent strategic plans to fully leverage the SOF-like capability.

Finally, there is always the prospect that a state actor from outside the region might take an interest in the outcome of this conflict between two non-state actors over an "ungoverned" part of that region. That state actor might favor one non-state actor over the other, and could elect to contribute elements of its own special forces to tip the outcome of the conflict in favor of its chosen side. Thus, as more and more non-state actors begin to demonstrate the ability to shape the international environment at the strategic level, we should to see more direct involvement of major state actors in the struggle between the non-state actors.

Force Requirements

With the Hutus and the Tutsis building their special operation-like forces, their size, scope and capacity will grow, and their ability to influence events at the strategic level would increase as well. Both sides would need to buttress their recruiting and training to develop more skilled SOF-like forces. Simply giving AK-47s to 15-year olds would be insufficient to create a SOF. Both sides would likely also invest in, and embrace, any technology that increases the chances of mission success and operational effectiveness, with examples ranging from the UAVs to C4ISR equipment to increasingly sophisticated IEDs. For example, with the growing ubiquity of UAVs, and the rapidly falling prices, both sides would have sufficient financial resources to acquire a wide range of reconnaissance and strike UAVs. Moreover, each side might turn elsewhere to acquire intelligence data; for example, images from commercial satellites could be leveraged extensively.

V. A *Renaissance* in Strategic Warfare

"In cases of defense 'tis best to weigh the enemy more might than he seems."

--- William Shakespeare

The Prospect of a Renaissance

The future international security environment that is unfolding is potentially unprecedented both in its complexity and in the degree of challenge it presents to the dominant power – the United States. Instantaneous global communications and social media will progressively allow less powerful states and, non-state actors, to compete more effectively with the most powerful of nation states. Global economic and financial interdependence and interconnectivity are the mainsprings of world prosperity but their single-point failure nodes are vulnerable to cyber and/or space attacks and to pre-planned 5th column electronic saboteurs. Political stability and legitimacy can be undermined by strategically focused hyper communications campaigns which seek to displace the established societal narrative with one favoring the insurgents or a hostile opposing state. Physical attacks against selected high value targets no longer may require massive bomber or missile strikes but can be achieved by either terrorist strikes on the part of non-state actors or by focused Special Force operations conducted by states within established norms of war.

In combination, these developments open the possibility of a new dimension of conflict and war – one that lack commonly understood front lines, massive air campaigns, or large amphibious landings. It is becoming progressively more possible to attack the enemy's center of economic and political gravity (and to a considerable extent even his direct military potential) without engaging his carefully deployed military forces. As a result, non-state actors, lacking armed forces as traditionally understood, have the potential of effectively striking even great powers. And lesser states, which are unwilling or unable to develop effective traditional militaries can now avail themselves of options to more effectively engage their rivals or even the world's major military powers without bothering to develop military forces as traditionally understood. Such powers, in fact, can "rent" rather than develop their own cyber warfare capability by recruiting hackers, and perhaps even mainline programming specialists, attracted by high enough salaries and by the challenge of penetrating firewalls of the world's greatest powers. These cyber mercenaries already have an existing parallel in the current cyber-criminal world where expertise, techniques, and purloined financial access data is freely, if expensively, available. On the higher end of the moral spectrum, the purchase of such cyber capabilities by an established state can be internationally justified as being no different than the existing practice of buying space lift capability by nations able to develop satellites but not space launch vehicles. The covert recruitment of these mercenaries would be particularly attractive since

they can conduct a coordinated cyber campaign from diverse locations thus further complicating the task of locating the source of the attack. This transcendence of the historic requirement to possess effective military power in order to shape the global narrative or/and strike at the opponent's key national assets and values suggests that we may be entering a period of a renaissance in strategic warfare.

Change is also occurring within the traditional areas of military completion. Access and anti-access regimes –descendants of the precision strike capabilities of the Revolution in Military Affairs (RMA) are successfully eroding nation-states' power projection capabilities. Progressive advances in autonomous robotics, nanotechnology, highly inter-connected, continuously converging computing capabilities, additive manufacturing, and human augmentation present steep challenges to the viability of the legacy *Few, Expensive and Manned* weapons systems.

These trends and developments are forming a *multi-dimensional, multi-player, and multi-threat* security environment whose cumulative nature and lack of established rules and practices only accentuates the challenges facing the nation states. Adapted and exploited correctly, these trends have the potential to enhance the power of the nation-states through reliance on the *many, cheap, and unmanned* military capabilities, thus laying a foundation for a Renaissance in strategic warfare. Failure by a nation state to successfully address these developments suggests progressive erosion of its relative global power capability and for a great power like the U.S. a growing inability to shape and develop the global narrative to its advantage.

In contrast, an interesting aspect of the Cold War was not only its division of the global community into binary camps but also the submergence, often by American or Soviet fiat, of local conflicts and aspirations. True, the non-aligned movement emerged early and, on occasion, did handicap the execution of US foreign policy. Nor were all local conflicts totally eliminated and as the bi-polar system wore down with age, the temptation to employ proxies to further great power objectives became more difficult to resist, witness Angola, Mozambique, and Afghanistan. But the power of the binary actors was paramount – they shaped the international security environment by their monopoly over the global agenda, their military potential was unrivalled by alternative sources of power; and the US enjoyed a significant asymmetric advantage in its ability to project global power. The emerging national security environment shows signs of reversion to a more classical model of multiplicity of (not necessarily equal) players, often unchecked regional crises and conflicts, a lack of even an appearance of control by the great power over the global agendas, and a progressive erosion of US power projection capabilities. The end of the Cold War and of a nuclear armed truce was certainly the precipitating event but these trends are now more powerfully fed by the extraordinary growth in global hyper-communications and social media and by the action-and-reaction cycles of competition associated with the advanced technology trends affecting warfare.

These complex interrelationships within and between these, and related, technological trends produce unexpected and unpredicted capabilities, opportunities and threats which nevertheless affect both the players in and the nature of the international competition. These emerging trends are not a revolution insofar as they are no longer fully directed and controlled by nation-states but rather arise out of the technological and social environment itself. Thus,

hyper-communications and social media support a *Renaissance* in a multi-dimensional, multi-player, and multi-threat international security environment. Progress in robotics and nanotechnology, for instance, in response to precision strike weapons, suggests these systems may be victims of their own success and that the new paradigm of *Many, Cheaper, and Unmanned* could result in a *Renaissance* in more unfettered US power projection capabilities. Finally, cyber and space warfare permit not just weaker states but also some non-state actors to bypass the military forces of a powerful opponent and to directly strike his economic, political and even social infrastructure leading to a *Renaissance* in homeland-to-homeland strategic warfare.

Current Trajectory

Despite the current age of extraordinary technological and social change the international security environment resists rapid change, thus the next decades are likely to exhibit important continuities with today. Globalization will continue to enhance national economies, especially in the Far East and India, providing capital, technology, and appropriately socialized citizenry to support progressively more modern and effective military establishments. The RMA- conceived by Soviet planners and brought into fruition by American strategists and technocrats is ever more in the center of military planning and operations. The implications of the concept of "if you can see them, you can hit them" is now a more globally understood phenomenon. More importantly, the proliferation of long range, highly accurate, and destructive weapons systems is creating a progressively more effective anti-access regimes which threatens a key US core competence -- global, timely power projection. While not necessarily fully equal to the US military, progressively more states will be capable of challenging American power projection capabilities in their own home waters as a way to increase the costs of American operations and thus decrease the odds that the campaign would be initiated in the first place.

To retain a broad range of power projection capabilities, DOD leadership faces a daunting challenge of maintaining a dynamic balance between mainlining RMA concepts and systems (already approaching middle age), the legacy forces which are still vital for operations not involving force projection, and increasingly important hyper-communications, cyber and space warfare capabilities which are cumulative to the other two in terms of capabilities and risks. Expected progress with robotics platforms -- both remotely and autonomously operated -- miniaturization via nanotechnology, energy and critical subcomponent generation/production in the field, and advances in biotechnology and human augmentation is likely to produce weapon systems and associated technologies which could result in the fielding of smaller, more agile, more supportable, and more survivable forces capable of penetrating anti-access regimes at costs that may be acceptable to the national leadership.

Potential for a Renaissance for U.S. Power Projection Capabilities

More difficult to assess is how these new capabilities will be integrated into the Services in terms of doctrine, organization, and training. If added cumulatively to the existing structures and functions, the new capabilities will enhance US ability to project force in an anti-access environment while reducing human and material costs but at a risk of creating an unending

see-saw action-reaction cycle between the attackers and the defenders. But if the new capabilities, some of which are likely to be revolutionary, are used as a basis for evaluating how we can alter the current dominant paradigm of war, then there is a real potential for a revolutionary change no less significant than the one associated with precision strike systems.

The key to developing more effective tactics and operation art rests with a willingness to repeat the practices of the inter-war period and conduct large-scale experimentation a la the Wehrmacht's Kriegsspiel and field exercises that validated the concept of Panzer Divisions and US Navy Newport War Games, which laid the foundation for US resurgence and victory in the Pacific. Effective new paradigms hold the promise of retaining US power projection capabilities in the face of ever more effective precision strike regimes and of supporting and successfully operating far smaller expeditionary forces required to survive on an ever more transparent battlefield. The ability to operate at will in a fully saturated anti-access environments would signal a *Renaissance* in US force projection capabilities harkening to the pre-precision era of unfettered access, limited primarily by possible reactions of other great powers.

Multi-Dimensional Security Environment

A new and complex challenge to US military capabilities lies in potential future missions to protect American and Allied national assets far away at sea -- the Arctic, the Antarctic, the South Atlantic, the South China Sea, and the Pacific are likely to become potential future areas for specialized undersea operations.

Global economic growth will continue to place greater demands on available supply of energy (still primarily oil and gas in terms of potential for conflict) and critical minerals (not only 'rare' earth but also assured access to deposits such as copper and bauxite) which despite enhanced exploitation technology and the discovery of new deposits are likely to produce periodic transitory but still economically dysfunctional shortages and price spikes. The search for new deposits will steadily expand into deep ocean areas aided by improvements in existing robotic platforms which will permit the exploitation of ever deeper energy and mineral deposits.

Given the remote location of some of the likely deposits, the often untested applicability of the Law of the Sea, and historic practices regarding unsettled territorial disputes there is a high likelihood for crises and even conflict. Consequently one can expect the development of deep diving remotely controlled and autonomous robotic platforms capable of patrolling and, if necessary, defending nationally claimed under sea natural resources. The technologies developed for this realm and those associated with access and anti-access strategies will most likely cross pollenate, for instance, development of long-duration, autonomously operating armed underwater craft to sanitize and maintain security of areas used for sea-borne force projection.

Some Trends Persist

Not all challenges will be new nor all will require new weapon systems and technologies. For at least the near term future Beijing's significant concern for and desire to secure Chinese lines of economic communication presents an unique source of tension and even potential conflict.

Distrusting the United States' guarantee to safeguard freedom of the sea to one and all, the Chinese seek a true blue water navy and a global presence to safeguard and enhance, if necessary, their national interests. The rise of a new global power is inherently destabilizing as the power balance is recalibrated, increasing, at least temporarily, the risks of miscalculation in a crisis or from confrontations stemming from the Beijing's Imperial overreach. Traditional naval presence, involving legacy systems, appears to be still required to assure freedom of the sea to the international community and to serve as a hedge against a range of possible future Chinese actions.

Multi-Actor Security Environment

The developments in hyper communication, social media, cyber and counter cyber capabilities, and space warfare hold potential for a rapid and a drastic national security paradigm shift and even the potential for *Renaissance in Strategic Warfare*.

A signature new feature of the future security environment is the ability of a wider array of actors, and even individuals, to set the agenda of the international community in ways that limit or force the options of nation-states.

The post-Westphalian nation-states, a system which acquired near-global status in the post WW II period, has been challenged by non-state actors before but their reach, capabilities, and staying power were not sufficient to dislodge the centrality of the nation-state. The dissemination of affordable and reliable methods of direct and rapid communication first made possible the popular overthrow of the Marcos government and later bloomed into the color revolutions of Central Asia.

The pervasiveness of hyper communication and social media, combined with the difficulty facing modern nation-states in suppressing these capabilities without undermining the vitality of their own information based economies suggests that the newly found potential of non-state actors is likely to persist into at least the mid-term future. More importantly, as more players begin to directly influence and define the international agenda, the very concept of "suppressing" becomes problematic.

It is certainly theoretically possible for a government to attempt to control and limit but not totally deny its citizen's access to web-based resources and social media outlets. In fact, the Chinese government's massive efforts to control the political content of its citizens' communications provides a real time laboratory for the study of the potential of sub-national actors to affect social and even regime change. While evidence suggests that the government has had some success, it is also known that social media participants are able to employ analogies (often from China's mythology and history) to avoid triggering controlling algorithms, with the more adept web surfers being able to circumvent the "Great Firewall" which in theory protects China against the harmful outside world. While these skirmishes between the authorities and their "electronic citizens" continue, the real test of the system will only occur in the event of a systemic crisis involving significant social disorder -- a scenario which is likely to present Beijing with Hobson's choice of disconnecting from the Internet (and thus precipitating an economic crisis in its progressively interconnected economy) or losing the information

battle. And, it should be noted that Beijing's commitment to and resources lavished on its so-called Great Firewall of China are highly unlikely to be matched by other states suggesting considerable future freedom of action for non-state actors.

The potential of non-state actors is further enhanced by the vast difference in the power, stability, and effectiveness of states along the continuum depicted in future Figure X. *Nation-states*, such as the United States, France, Germany, China, India, Turkey, Brazil and South Africa, have a history, elite culture, political structure and language policies that underscore their unitary (but not necessarily homogenous) nature; in theory, nation-states have the most comprehensive military and economic wherewithal to combat non-state actor threats, though non-state actors still pose an increasingly complex threat to nation-states. Alongside the nation-state are two additional categories of state actors at greater risk from non-state actors: *tribal states* and *dysfunctional states*. As described earlier, tribal states (for instance, Iraq and Pakistan) are entities whose history of wars, colonization and decolonization did not produce an organic unitary state but rather one that is composite in nature, with regionalism and tribalism being the dominant societal forces. Their unity and effectiveness varies but they offer a range of polities which are more susceptible to attacks by non-state actors. Dysfunctional states (for instance, Afghanistan, Yemen, and Mali) are the most challenging; their inherently weak central governments and internal struggles for power are both sources of global instability and rich targets for intervention by non-state actors.

The resulting sanctuaries provide a difficult challenge to the traditions and practices of an international system based on nation-states. Non-state actors, whether politically or criminally oriented, seek, and often find, shelter behind the concept of national sovereignty -- a concept originally designed to allow a sovereign s to rule their subjects as they pleased and one that acquired far greater international legitimacy with the raise of global nationalism. For the terrorists and politically extremists the purposeful misuse of national sovereignty provides a safe haven from which to engage in and shape the global strategic narrative on par with nation-states. This unprecedented sharing of the global dais with great powers provides additional credibility to the non-state actors in the eyes of their targeted audience—the self-perceived marginalized sectors of developing societies. The non-state actors also benefit from the fact that governments are by nature ill-suited to effectively deal with today's fast paced, dynamic media forums thus being less effective in shaping the global competitive narratives. Yet, international norms are not immutable to change and it is clearly unwise to unthinkably apply concepts which may have become outdated by reality. If non-state actors function as peers in the setting of global agendas, they are logically subject to the same sanctions as nation states. Nor can it be acceptable that they enjoy the protection of international norms without accepting their corresponding responsibilities. Thus, the concept of the right of humanitarian intervention used against states like Libya suggests that a non-functional state too could be viewed as endangering the international community by its inability or unwillingness to exercise national sovereignty. Consequently, internationally based intervention to restore order to safeguard international security would be appropriate and justified.

Emerging Threats – Emerging Opportunities

The inherent weakness of tribal and dysfunctional states suggests that even a spontaneous reaction to a local outrage or to a long-simmering issue can be (as by now repeatedly shown) a superb organizing force to mobilize, via hyper communication and social media, large numbers of people against a regime or a specific group -- a process aided by the lack of effective and legitimate sources of central power. The issues in the near term could be a demand for a representative government, a return to a 'golden age' of theocratic rule, or the repression of corruption which resonate with the population at large and whose massive public demonstration of their demands paralyze their societies and produce customary outrages on the part of the security forces. But very soon the issues could elevate to those that influence, and in some ways, help define the strategic narrative. The subsequent galvanization of the international opinion, immeasurably aided by global communications, constrains the freedom of action of the dominant nation states forcing, at the very least, expenditure of resources to support diplomatic efforts to stop the outrages, with increasing risk of direct military involvement in a campaign over issues of international norms rather than core national interests, including straining ties with long-standing allies.

At the further end of this spectrum are terrorist and extremist groups who have shown a high degree of adaptability to new technologies to further their goals. There is no reason to think that they will fail to capitalize on the advances in nanotechnology, adaptive manufacturing, and human augmentation to move even further down the road to political objectives. These technologies will be a tremendous force multiplier for these well-organized institutions which probably already are exploiting the wide array of methods open to them not only to seize an opportunity for social mobilization offered by the deeds and the misdeeds of the ruling elites but also to play on the very ethnic and regional difference that can turn tribal and dysfunctional states into areas of chaos and lawlessness. These areas offer ideal bases for terrorist groups by providing operational freedom, sources of income and of recruits, and serving as vivid demonstrations of the extremists 'successes' against the established international order. In addition to the issues of national sovereignty, the risks and costs of intervention serve as formidable barriers to action on the part of the nation-states. The lack of success in cases such as Somalia and Sudan merely underscores the opportunities for non-state actors to damage the established international order and the limitations facing nation-states, when they are forced to deal with effective non-state opponents. Nation-states, historically structured to interact primarily with similarly structured unitary actors, will need to develop new strategies, perhaps reaching into history for examples of the use of auxiliary and allied forces, to more effectively deal with this new international reality.

One consequence of this development for the US is the loss of primacy enjoyed previously by great powers in setting and pursuing their global agenda. As a result it would be prudent to comprehensively assess which areas are at a high risk for non-state actor scenarios and to preplan a range of appropriate US responses. This, at the very least, will reduce the chance of being forced into situations by the flow of events and having to deal with the diplomatic, economic, and potential military costs and risks on an ad hoc basis.

Perhaps most importantly, non-state actor-generated events can no longer be viewed as one-off occurrences which the US can dispatch with ease and return to its more central geo-political pursuits. Furthermore, it would be prudent to assume that Al Qaeda's successors or hostile states acting through terrorist proxies will consider preparing comprehensive campaign plans designed to generate or to exploit incidents capable of causing mass societal unrests in areas of interest to the US. These campaigns would be viewed as cheap, deniable, and potentially highly effective means for undermining American allies or/and as means of diverting Washington's attention and capabilities away the actual areas where the aggressor wished to expand his influence or control.

The ability of non-state actors to affect not only American international agenda but also to threaten directly US regional interests and the integrity of its key allies presents a particularly difficult set of challenges. In addition to the issues of international legality, host dysfunctional states (and, in the case of Pakistan, tribal states) may very well possess anti-access capabilities which have the potential to significantly increase the cost of force projection. The concentration of US and Allied naval power and the build-up of massive land bases to support operations of the *Few, Expensive, and Manned* systems provide a rich target set not only to the dysfunctional state (committed to preserving its sense of independence) but also to non-state actors. The variety and availability of anti-accesses systems, and progressively cyber warfare capabilities, provide select non-state actors with capabilities equal to those available to them in the realm of social media. The development and introduction of military capabilities based on the principle of *Many, Cheap, and Unmanned* offers the possibility of shifting the dominant paradigm of war to permit nation-states, their allies, and their auxiliaries to operate successfully in anti-access environments.

Multi-Threat Security Environment

Another and perhaps most revolutionary aspect of the non-state actors gaining measurable geo-political heft is the fact that very technology that has enabled them to be more significant players has the potential to be turned much more directly against the very industrial world that has created it.

While the nation-state is no longer unchallenged, it remains first among equals in its ability to organize and focus societal financial, economic, technological, and demographic potential for the defense, and sometimes the expansion, of its national interests. The nation-state's techno-economic organizational ability has been and is increasing as a result in the continuously improving communication, computing, and data management capabilities. To be competitive in the face of great disparity in international wage structures, the leading economies, including the US, have become depended on complex global links supporting 'on demand supply' (to reduce inventory costs) and robotization (to reduce labor costs). Superbly efficient in peace, this interdependent economic system has significant potential vulnerabilities in crises and in war which could be exploited by rival states and even by some non-state actors.

Economic globalization, especially its reliance on highly integrated communications, shared data bases, and remote, automated machine control networks creates system wide

vulnerabilities which could allow for another option for homeland-to-homeland "exchanges", without involving, for the bigger powers, nuclear weapons, thus heralding a potential *Renaissance* in strategic warfare.

The Evolution of the Art of War

While operational art focused on the destruction of enemy forces by fire, shock, or maneuver, the equally important war termination strategies focused on the seizure or destruction of the enemy center of gravity. At its classical best, the concept is illustrated by Alexander, supported by his Companions, charging directly at Darius - the center of a tyrannical system that could not (and did not) survive his death. As kings grew loath to take the field and states became more complex and thus more capable of surviving the loss of a leader, the capture of the hostile capital became the objective, a strategy which reached its apex in the Napoleonic and the American Civil Wars. Nevertheless, the destruction of the enemy's forces both in the field and in reserve remained a vital requirement as witnessed by Napoleon's icy retreat from burned out Moscow (harried by the resurgent Russian Army) and his eventual defeat. This was not a mistake repeated by Grant whose destruction of the Confederate forces defending Richmond permitted the imposition of an unconditional surrender.

The rise of military aviation and a desire to overcome trench warfare permitted attacks against the enemy homeland and his economic potential before the destruction of his forces but the strike capabilities of the Gotha and Zeppelin raids of WW I, while of considerable psychological value, were not sufficient to materially alter the course of the war. The inter-war period saw concerted interest in the development of air warfare doctrines which offered the possibility of destroying the economic potential of the enemy by strikes against his homeland and thus destroying the ability of his forces in the field to continue combat. Massive bomber strikes of WW II certainly significantly damaged German and Japanese war industries, thus contributing to their defeat but the prolonged and expensive in manpower air campaigns (mainly the result of inaccurate ordinance) did not result in the rapid destruction of the enemy capability and will to fight. Only the advent of nuclear weapons offered the immediate destruction of the enemy's political and economic centers of power but at the high risk of equally destructive counter-strikes.

A Renaissance in Strategic Warfare

The rules of the Cold War permitted wars on the periphery and wars by proxy but the integrity of the homelands was central to the concept of the nuclear deterrence -- an attack on one's Zone of Interior was widely viewed as risking the initiation of limited or even full-scale nuclear exchanges. But now the combination of rapid, assured global communication, coupled with the ever growing capabilities of cyber warfare makes possible highly effective, rapid, and continuous strategic strikes against an enemy's political, military, financial, economic, and even social centers of gravity. Focusing on the economy, the interface of the global information grid with physical control system, global supply chains, and single-link production and distribution systems offer extraordinarily rich targets for cyber warfare in terms of electronic strikes from abroad, initiation of pre-planted viruses, and 5th column electronic saboteurs. As an example,

properly focused attacks on a nation's electric distribution grid can cripple the system and result in a rapid shutdown of its economy, with the restoration of that capability potentially being a long and difficult task. Similar attacks on an opponent's political and military key nodes are both possible and desirable. Against less capable military powers, particularly those not capable of directly striking the attacker's homeland, select SOF strikes against space, energy, and command nodes located near shorelines and land borders offer considerable advantages but which will need to be considered against the potential risks of escalation and counter strikes against one's regional assets and allies.

Such strategic attacks on an opponent's homeland by a nation-state could be accompanied by the initiation of space warfare against his key satellite capabilities. The previously discussed consequences of the degradation of GPS services highlight the extent of economic damage that would result. Attacks against vital space assets and the appropriate counter measures to protect them is clearly an important issue but one, as is the case of a more detailed discussion of cyber warfare, would need to occur in a different, classified forum. What is possible to note is that the opening of space as a domain of focused and sustained warfare creates a new dimension of strategic warfare -- an opportunity for an opponent to indirectly but extremely effectively strike at the economic and social infrastructure of the enemy, figuratively over his forces in the field, without necessarily evoking sanctions associated with the Cold War.

Davids and Goliaths

In a dramatic departure from norms of previous epochs of strategic warfare, some non-state actors are likely to have limited cyber attack capabilities against select terrestrial and space assets of nation-states. Such attacks would not be comprehensive in nature nor seek to collapse the economy of the victim state. Rather, such attacks would constitute super 9-11s designed to maximize symbolic and political goals of the terrorists, including the forcing of nation-states to negotiate, and even accommodate, the non-state actors as if they were state entities.

US response to such an attack would be complicated by a myriad of issue. In addition to the difficulties associated with interagency coordination there are significant questions relating to federal-state-and local jurisdictions, corporate proprietary rights, and personal Constitutional guarantees. Furthermore, it may be difficult to locate the actual source of the attack since it would like be launched using 'captured' or 'zombie' computers organized in massive botnets to both hide the identity of the attacker and to maximize the effectiveness of the attack. A key factor to stress is the likelihood that such an attack will not be a 'one-off' attack but potentially represent a series of attacks - a virtual campaign. And, the destruction of one such opponent would not preclude another from repeating this form of an attack at a different time. A full assessment of this threat lies in the intricate and closed world of cyber warfare but on the policy level the key appears to preemptively eliminate 'safe areas' from which such attacks could be launched and, failing to prevent an attack, coercing, if necessary, the willing or the unwilling host nation to permit the use of outside forces to destroy the threat.

Expanding the State-on-State Conflict Spectrum

On the state-to-state level, the ability of a hostile nation-state to directly challenge the US without the burden of developing a force structure which could compete, at least in principle, with US forces is revolutionary in itself. That such an aggressor could, for the first time in history, simply bypass US forces in the field and strike directly at the heart of the US homeland suggests that homeland-to-homeland exchanges, moribund in the nuclear age, may experience a *Renaissance* in terms of credibility and effectiveness. And the attractiveness of this form of warfare is enhanced by the fact that far more nation-states (and some non-state actors) are capable of developing offensive cyber capabilities than those capable of slowly nurturing combat forces capable of standing up to the US military.

The Nuclear Dimension

Such attacks on the US would entail a high risk of retaliation on the homeland of the aggressor. On the high end of the violence spectrum, the US NCA retains the option of authorizing nuclear strikes either (or perhaps both) for retribution or to prevent follow-on massive cyber attacks. The release of nuclear weapons would be highly scenario dependent. For instance, one would expect that the US willingness to use nuclear weapons would depend whether or not the cyber strike proved to be a precursor of a more general attack; or if it was seen as a calibrated and calculated step up the escalatory ladder in the course of an ongoing conflict; or if it was perceived to be a desperate last gamble by a regime intent solely on its own survival. No less important will be the state of mind and the personal calculus of the President -- one can easily draw up persuasive arguments pro and con on the part his, most likely divided, advisors.

A very important continuity in the cyber warfare age will be the distinction between nuclear weapons states and the rest of the world community. Nuclear weapons will retain their status as 'the final answer of the king', particularly in their traditional role of deterring aggression, either initial or subsequent, by holding at risk those assets and values that the enemy holds dearest. One could envision retaliatory strikes directed only at the leadership that initiated the cyber strike against the US or another nuclear power. The objective of such a strike would be to retaliate against the actual guilty parties, sparing, as much as possible, their societies which perhaps were unwilling participants in the original attack. In such scenarios the development or non-development of follow-on clean nuclear weapons is likely to play a decisive role.

New Game Requires New Capabilities

It would be argued that a cyber counter-strike would be the appropriate and proportional response. That may be the case if appropriate cyber attack plans exist, or could be rapidly developed, against the aggressor state. One consideration will be whether or not the initial cyber strike was able to degrade enough of the US capabilities to delay a counter-strike sufficiently long for the aggressor to achieve his specific geo-political goals and present the US with a fait accompli. Another, interesting consideration is the possibility that an aggressor would maximize his own protection prior to launching a cyber strike and, in fact, disconnecting, temporarily, his entire network of systems in order to first judge the effectiveness of the US cyber response.

The Role of Forward Forces

Of course, the attacker could be vulnerable to severe strikes by the US forces in the field and those generating forward from the homeland. The ability to even significantly degrade the economic, political and social domestic framework of an enemy does not immediately paralyze his force. The failure to account for the latent capabilities of the forces in the field will continue to risk repeating Napoleon's fatal error in failing to destroy the opponent's actual rather than potential military capabilities.

Consequently, an attacker who would be willing to risk US nuclear retaliation, is highly likely to attempt to at least temporarily immobilize deployed US forces by also directing cyber strikes against their capabilities as part of a general attack on the US. Such an attack could be complimented by sabotage, electronic and physical, as well as surprise missile strikes against key control nodes. The remaining US force capabilities would be absorbed by the aggressor's anti-access capabilities in littoral waters, by strategic air defenses, and by target denial through mobility, dispersal, or underground sheltering.

U.S. Offensive Options

While defense against cyber attacks is likely to present formidable challenges, due to the complexity of the threat and the nature of American society, there are considerable possibilities for US offensive cyber capabilities. The nation's rich techno-communications infrastructure, a population well versed in social media, and a Departmental commitment in the form of a specialized Cyber Command speaks to the potential complexity and effectiveness of offensive cyber tools that could be available.

But the employment of such a strategy would need to resolve considerable policy, interagency, and socio-political issues. Furthermore, US moral repugnance of surprise attacks would preclude the use of cyber in a precursor attack.

One can envision the US responding to a homeland cyber attack or being engaged in a prolonged access versus anti-access campaign employing a combination of cyber attacks, space warfare, and SOF strikes to achieve conflict termination as a way of preventing additional mutual losses. The use of cyber and space warfare capabilities would be undertaken to support US theater operations, bypassing the opponent's anti-access capabilities, and directly attacking his socio-economic base not only to reduce his ability to support his forces but also as a means to erode his willingness to continue the conflict

Even if the opponent elects to continue, the combined campaign will significantly reduce his ability to support his anti-access forces, allowing them to be more easily destroyed. A key advantage of such a campaign, in addition to avoiding hostile domestic and international reactions as a result of collateral damage, is its ability to be conducted in a way that minimizes (or eliminates) reliance on in-theater bases, on local allies, and on large concentrations of potentially vulnerable naval forces.

Opportunities, Costs, and Risks

The emerging trends support a *Renaissance* in US global strategic warfare capabilities by providing the NCA with credible, non-nuclear options against an opponent's homeland to deter and if necessary reverse aggression at an acceptable cost. While the opportunities are great so are the challenges facing the US in fully realizing its potential. For instance, the difficulty in defending against cyber attacks, especially against non-state actors, underscores the disadvantages facing a dominant nation-state like the US in dealing with a security environment where even its nuclear forces do not provide the same level of protection against a homeland attack. Furthermore, the transformation of US forces to overcome anti-access regimes in order to realize a *Renaissance* in force projection faces significant organizational, doctrinal, and financial challenges.

Despite the challenges, US successes in these fields would mark a paradigm shift which will favor the maintenance of American military predominance in the period in question. And while the new security environment generates opportunities and threats which are cumulative to the existing baseline, the costs associated with the development and deployment of future capabilities based on *Many, Cheaper, and Unmanned* systems, particularly when they are organized in ways to maximize their effectiveness, are not cumulative. Such new capabilities offer greater trade-off opportunities between and among systems, particularly as technology is leveraged to reduce manpower costs. Taken together with lower procurement costs, particularly for unmanned platforms and for replacement of systems lost in battle, suggests the possibility that the future cost-benefit analyses may prove to be favorable. And since these trends and their attendant consequences are no more stoppable then Canute's waves, we may be wise to follow Churchill's advice and to begin comprehensively analyze, plan, and prepare to exploit the opportunities and hedge against the risks offered by this future.

Bibliography

Books / Reports

Akanda, Ali Shafqat, and Justine Treadwell. “Contributing Factors in the Ongoing Water Conflict Between Bangladesh and India.” Tuffs University, March 2009.

Alston, Philip. “Non-state Actors and Human Rights.” *Academy of European Law.* New York: Oxford University Press, 2005

Alterman, Jon B. and John W. Garver. “The Vital Triangle: China, The United States and the Middle East.” Center for Strategic and International Studies. 2008

Asprey, Robert “War in the Shadows: History of Guerrilla Warfare.” New York: William Morrow & Co; 1994

Chaliand, Gerard. The Art of War in World History: From Antiquity to the Nuclear Age. University of California Press, October 7, 1994.

Cronin, Richard and Timothy Hamlin. “Mekong Tipping Point.” Stimson Center, 2010.

Esarey, Ashley. *Testimony before the U.S.-China Economic and Security Review Commission.* Hearing on ‘China’s Narratives regarding National Security Policy.’ U.S.-China Economic and Security Review Commission. March 10, 2011.

Jones, Archer “Western Way of War.” Chicago: University of Illinois Press, 2000

Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China* 2010, Washington, D.C, 2010,

Ofori-Amoah, Abigail “Water Wars and International Conflicts.” University of Wisconsin, Eau Claire, USA, Spring 2004.

Rath, Thomas J. “Tools of change: tactical C4ISR and conflicts--past, present, and future.” *Air & Space Power Journal.* U.S Air Force: Gale, Summer 2011.

Rosen, Stephen P. “Winning the Next War: Innovation and the Modern Military.” *Cornell Studies in Security Affairs.* Ithaca, NY: Cornell University Press, 1994.

Similla-Gonzales, Francis Robert. “Reinscribing Dominant Narratives of the ‘Other.’” *Brown University*, April 15, 2011

Smith, Adam. *Wealth of Nations,* edited by C. J. Bullock. Vol. X. The Harvard Classics. New York: P.F. Collier & Son, 1909–14; Bartleby.com, 2001.

Articles

Abrahamsen, Rita and Michael C. Williams. “Securing the City: Private Security Companies and Non-State Authority in Global Governance.” *Mercenaries, Pirates, Bandits and Empires: Private Violence in Historical Context*. B. Mabee and A. Colas (eds), New York: Columbia University Press. (2010)

Alamy, “Print me a Stradivarius: How a new manufacturing technology will change the world" *The Economist,* Feb 10th 2011,

Avant, Deborah. "The Privatization of Security and Change in the Control of Force." *International Studies Perspectives* 5.2 (2004): 153-157.

Connor, Michael J. "Investing in the Undersea Future." *U.S. Naval Institute Proceedings* 137.6 (2011): 16-20.

Corum, James S. "Future Battlespace and the US Response." *Baltic Security & Defense Review* 11.2 (2009): 21-39.

Franz, Timothy. "The Cyber Warfare Professional: Realizations for Developing the Next Generation." *Air & Space Power Journal* 25.2 (2011): 87-99.

Junio, Timothy J. "Military History and Fourth Generation Warfare." *Journal of Strategic Studies* 32.2 (2009): 243-269.

Hamblins, David, *“GPS Chaos: How a $30 box can jam your life.” New Scientist* (web) 21:06, March 6, 2011.

Libicki, Martin C. “The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon” McNair Paper 28 (Washington: National Defense University, 1994)

Mandhana, Niharika. “Water Wars: Why India and Pakistan Are Squaring Off Over Their Rivers.” *Time,* April 16, 2012.

Rai, Neena. “Water Wars May Lie Ahead.” *Wall Street Journal,* June 29, 2011.

Potenziani, Ernest. "Current and Future Trends in Military Electronic Warfare Systems and the Role of Thin Films and Related Materials." *Ferroelectrics* 342.1 (2006): 151-161.

U.S. Geological Survey. “90 Billion Barrels of Oil and 1,670 Trillion Cubic Feet of Natural Gas Assessed in the Artic.” USGS Newsroom, July 23, 2008

Walker, Jeffrey K. "The Demise of the Nation-State, The Dawn of New Paradigm Warfare, and a Future for the Profession of Arms.” *Air Force Law Review* 51. (2001): 322.

Wilkie, Robert. "Hybrid Warfare Something Old, Not Something New." *Air & Space Power Journal* 23.4 (2009): 13-17.

Work, Robert O., and F. G. Hoffman. "Hitting the BEACH in the 21st Century." *U.S. Naval Institute Proceedings* 136.11 (2010): 16-21.

Digital Media

Adams, Thomas K. "Future Warfare and the Decline of Human Decisionmaking." *Paramaters* (Winter 2001-2002): 57-71. *Carlisle Army*. http://www.carlisle.army.mil/usawc/Parameters/Articles/01winter/adams.htm

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *International Policy Department*. RAND, 1993. http://www.angelfire.com/az/sthurston/Cyberwar.html

Avant, Deborah. "Private Security Companies." *New Political Economy* 10.1 (2005): 121-131. *T & F Online*. http://www.tandfonline.com/doi/abs/10.1080/13563460500031297

Blinkena, Anthony J. "Winning the War of Ideas." *The Washington Quarterly* 25.2 (2002): 101 104. *T & F Online*. http://www.tandfonline.com/doi/abs/10.1162/01636600252820162

Bloomberg, China, Brazil Agree to $10 Billion Loan, Exploration, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a1BzJNEdbjsc

Bousquet, Antoine. "Chaoplexic warfare or the future of military organization." *International Affairs* 84.5 (2008): 915-929. *Wiley*. http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2346.2008.00746.x/full

Brenner, Joel. "The Calm Before The Storm." *Foreign Policy.* 6 September 2011. http://www.foreignpolicy.com/articles/2011/09/06/the_calm_before_the_storm

Carafano, James Jay. "Thinking Differently About Winning Peace." 2007. *Heritage Foundation*. http://www.heritage.org/Research/Lecture/Thinking-Differently-About-Winning-the-Peace

Cebrowski, Arthur K, Vice Admiral, John J Garstka, and U.S. Navy. "Network-Centric Warfare: Its Origin and Future." *Proceedings* (Jan. 1998): n. pag. *Kinection*. www.kinection.com/ncoic/ncw_origin_future.pdf

Cohen, Joel E. "How Many People Can The Earth Hold?" *Discover.* N.p., 1 Nov. 1992. http://discovermagazine.com/1992/nov/howmanypeoplecan152

Cohen, Joel E. "How Many People Can Earth Hold? Well..." *Scientific American* . N.p., 21 Feb. 2011. http://www.scientificamerican.com/podcast/episode.cfm?id=how-many-people-can-the-earth-hold-11-02-21

Dahm, Werner J. A. "Technology Horizons; A Vision for Air Force Science & Technology During 2010-2030." *Technology Horizons*. U.S. Air Force, 15 May 2010. http://www.af.mil/shared/media/document/AFD-100727-053.pdf

El-Erian, Mohamed. "The Shape of the Global Economy Will Fundamentally Change." *Foreign Policy* (Sept.-Oct. 2011): n. pag. *Foreign Policy*. http://www.foreignpolicy.com/articles/2011/08/15/the_shape_of_the_global_economy_will_fundamentally_change

Finn, Peter. "A future for drones: Automated killing." *The Washington Post* 19 Sept. 2011: n. pag. *The Washington Post*. http://www.washingtonpost.com/national/national-security/a-future-for-drones-automated-killing/2011/09/15/gIQAVy9mgK_story.html ?hpid=z1

Gartenstein-Ross, Daveed. "Bin Laden's War of a Thousand Cuts Will Live On." *The Atlantic* (May. 2011): n. pag. *The Atlantic.* http://www.theatlantic.com/international/archive/2011/05/bin-ladens-war-of-a-thousand-cuts-will-live-on/238228/2/?single_page=true

Hirsh, Michael. "Home-Alone Economies." *National Journal.* 26 Sept. 2011. http://nationaljournal.com/home-alone-economies-20110926

Megacity Task Force, http://www.megacities.uni-koeln.de/index.htm

Parasuraman, Raja, Keryl A Cosenzo, and Ewart De Visser. "Adaptive Automation for Human Supervision of Multiple Uninhabited Vehicles: Effects on Change Detection, Situation Awareness, and Mental Workload." *T & F Online*. N.p., Apr. 2009. archlab.gmu.edu/people/rparasur/Documents/ParaCosdeViss09.pdf

Peters, Ralph. "The Future Of Armored Warfare." *Parameters* (Fall 1997): 50-59. *Carlisle Army*. http://www.carlisle.army.mil/USAWC/Parameters/Articles/97autumn/peters.htm

PriceWaterhouseCoopers, Mine 2011 The game has changed: Review of global trends in the mining industry, http://www.pwc.com/en_GX/gx/mining/pdf/mine-2011-game-has-changed.pdf

Rosling, Hans. "Hans Rosling on Global Population Growth." TED. July 2010. *TED*. http://www.ted.com/talks/lang/eng/hans_rosling_on_global_population_growth.html

Shachtman, Noah. "Inside the Freaky World of Next-Gen Night Vision." *Danger Room*. Wired, 14 Sept. 2011. http://www.wired.com/dangerroom/2011/09/night-vision/

Shachtman, Noah. "Tiny Pocketbots Prepped for Combat." *Danger Room*. Wired, 19 Aug. 2011 http://www.wired.com/dangerroom/2011/08/pocketbots/#more-54494

Shachtman, Noah. "After Lybia Shootdown, U.S. Robo-copter Will Weaponize." *Danger Room.* Wired, 18 Aug. 2011. http://www.wired.com/dangerroom/2011/08/after-libya-shootdown-u-s-robo-copter-will-weaponize/

Singer, P W. "PW Singer on Military Robots and the Future of War." Apr. 2009. *TED*. http://www.ted.com/talks/pw_singer_on_robots_of_war.html

Stockholm International Peace Research Institute. "Measuring military expenditure" http://www.sipri.org/research/armaments/milex/researchissues/measuring_milex

UNEP (2007) Global Environment Outlook: environment for development (GEO-4). UNEP. http://www.unep.org/geo/geo4/media

United Nations, Social Affairs, WORLD POPULATION TO 2300, 2004. http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf