HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

A NATIONAL DEFENSE FELLOW'S DEBRIEF FOR THE 2012-2013 ACADEMIC YEAR

LESSONS ON THE VALUE OF A MILITARY FELLOWSHIP, NORTH KOREA & IRAN'S NUCLEAR PURSUITS, AND THE EVOLVING CYBERSPACE DOMAIN

Lieutenant Colonel Troy L. Endicott
National Defense Fellow
United States Air Force

April 2013

Harvard University
John F. Kennedy School of Government
Belfer Center for Science and International Affairs
International Security Program

MENTOR

Dr. Steven E. Miller, Director, International Security Program
Belfer Center for Science and International Affairs
Kennedy School of Government, Harvard University

DISCLAIMER

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

CONTENTS

Abstract iii

Introduction 1

Lesson 1: The Value of a Military Fellowship 2

Lesson 2: Nukes, Still the Game Changer in a Post-Cold War Era 5

North Korea: The Precarious Nuclear Actor 6

Iran: A Nuclear State in Waiting? 13

Conclusion–Brief Lessons for the Military 19

Lesson 3: Cyberspace – The Domain Defining 21st Century Warfare 23

The Cyberspace Age and its Domain 26

Cyberspace and the Principles of Joint Operations 28

The People Element 38

Conclusion 41

Acronyms 44

Bibliography 45

ABSTRACT

This paper captures the thoughts of an Air Force fellow appointed by Harvard Kennedy School's Belfer Center for Science and International Affairs during the 2012-2013 academic timeframe. While events on the world stage during that time provided a military fellow with numerous opportunities for reflection and study, the paper briefly covers three topics of interest—a description of the author's fellowship and its value, how nuclear weapons are still "game changers" on the 50th anniversary of the Cuban Missile Crisis, and how the cyberspace domain is reshaping military activities and doctrine in the 21st Century.

The paper delves deeper into each topic and adds to an international relations dialogue by providing diplomatic, information, military, and economic considerations for dealing with North Korea's duplicitous yet credible nuclear threat and outlining incongruities in Iran's nuclear enrichment program and the dilemmas they present to the international community. Additionally in the cyberspace chapter, the author adds to an academic discourse by characterizing the cyber domain and key items of interest during the 2012-2013 period, especially enhanced Chinese cyber activities. In an effort to add to a military doctrinal discourse, the Principles of Joint Operations—Objective, Mass, Offensive, Maneuver, Economy of Force, Unity of Command, Security, Surprise, Simplicity, Perseverance, Restraint, and Legitimacy—are linked to cyber operations. Lastly, the paper emphasizes the 'people element'—the most significant factor that will define the success of a cyberspace revolution in military affairs.

INTRODUCTION

Each year, the USAF invests in 48 competitively selected, highly qualified senior field-grade level officers and civilian counterparts to participate in year-long fellowships within the Department of Defense, other government agencies, and distinguished civilian institutions such as Harvard University's John F. Kennedy School of Government.[1] Air Force senior officers attend these fellowships in lieu of residence war college programs (e.g., Air War College, National War College) and hone their professional skills before returning to military careers that entail senior staff positions within the Department of Defense, Joint Commands, service department staffs, and other post-squadron command positions.

This paper captures the thoughts of one of those Air Force fellows attending Harvard Kennedy School's academic think tank, the Belfer Center for Science and International Affairs during the 2012-2013 academic period.[1] *Simply put in military terms, this paper is one officer's 'debrief' of key lessons learned during a year-long academic fellowship.*

The following essays are stylized as thought pieces that dig deeper on pertinent lessons learned by the author throughout the year, specifically the value of a military academic fellowship, how nuclear weapons are still "game-changers" in a post Cold War world, and how cyberspace is defining military activities and doctrine in the 21st Century. These lessons are written for a reader with interests in international security, and are backed by scholarly reviews,

[1] The Belfer Center for Science and International Affairs was founded in 1973 as the Center for Science and International Affairs and has grown into the nucleus of Harvard Kennedy School's research in international security affairs, environmental and resource issues, and science and technology policy. The Belfer Center offers research and senior fellowship opportunities to nearly 70 distinguished scholars and leaders from the around the world. Two USAF officers are appointed as research fellows each year--one by the International Security Program and one jointly by the International Security Program and Project on Managing the Atom. Fellows work collaboratively with other center researchers and mutually support the Air Force Research Institute's goals to solidify relationships with civilian academic and policy communities, network with other fellows to broaden and develop senior leader competencies, and analyze current scholarly perspectives on defense policy and strategy issues.

opinions of leading internationalists and technologists, current military doctrine, and media reports.

LESSON 1: THE VALUE OF A MILITARY ACADEMIC FELLOWSHIP

Leading a 21st century military in a technologically and economically interconnected world requires practitioners to transition from tactical experts to organizational, policy, and strategic thinkers. While this might appear to be a statement of the obvious, a senior officer in today's military is often required to find opportunities to expand his/her mind, reflect beyond the battlefield and apply critical thinking skills to organizational, strategic, and national states of affairs. Chairman of the Joint Chiefs of Staff, General Martin Dempsey, describes himself as the "military's highest ranking student" and asserts, "Preventing wars and winning wars calls on us to outmaneuver our potential adversaries by outthinking them."[2]

Finding the resources for education is a challenge in today's fiscally constrained environment and shrinking force that requires its members to "do more with less" under the tyranny of a 24-hour clock. Nevertheless, in a sequester-weary era that threatens, among other things, tuition assistance for military members, a theme amongst professional officers remains the belief that education is the common foundation that buttresses the ingenuity and effectiveness of the world's most powerful all-volunteer force.

General Eisenhower described the value of learning and its worth when he said, "Education must always have a certain price on it; even as the very process of learning itself must always require individual effort and initiative."[3] Finding the time to study as a military leader is a worthwhile endeavor, but it requires extraordinary initiative when balancing the demands of family and mission. For example, a shrinking US Air Force has been at heightened

levels of war for over 20 years since Operation Desert Storm, but today still has 43 percent of the total force engaged each day in Combatant Command operations.[2] High operations tempos for deployed forces have placed additional burdens on those in garrison who organize, train, and equip them while juggling consistent inspection cycles and force shaping reductions. It is no wonder Air Force officers have little time to look past their own units, missions, and daily administrative demands to broaden their minds and think about maintaining the Air Force's decisive edge in an era of great change.

Fortunately, academic fellowships at institutions such as the Harvard's JFK School of Government allow officers to temporarily extract themselves from the rigor of a profession of arms and be exposed to environments that challenge their most basic beliefs and cultivate critical thinking beyond a tactical level. An undergraduate college professor of the author once described the value of an education is not necessarily what one learns, but how one learns to think. For officers who constantly think in the definitive, a fellowship provides an opportunity to think in the abstract. One learns to reason beyond "left and right" boundaries and recognize the nuances in between.

Another valuable piece of fellowships is the interaction an Air Force officer has with other fellows. For example, a Belfer Center Fellowship is unique in that two US Air Force officers are placed within a team of international 'up and coming' civilian scholars who are tackling very difficult concepts of international security in a globalized world, nuclear deterrence and proliferation, and technology-related policy implications. Valuable takeaways of the

[2] Between 1990 active duty end strength of 535,233 and projected active duty end strength for 2013 of 328,900, the Air Force will shrink 39%, well below end-strength totals of the Air Force in 1950 of 411,277 officers & enlisted members. Sources: "Air Force Almanac." *Air Force Magazine*, via the Web, and testimony by Hon Daniel Ginsberg and Lt Gen Darrell Jones to the Senate Armed Services Committee, Personnel Subcommittee. 25 Apr 2012.

interfaces include a profound understanding of other countries' perspectives of the current world order and specifically the leadership role of the United States and its military.

An establishment like Harvard's JFK School and its many institutes provide a smorgasbord of educational opportunities ranging from public policy and politics to international security. The author spent the 2012-2013 academic year focusing on subjects relevant to today's joint force, specifically the role of nuclear weapons in the 21st Century, the United States' role in the Middle East as it extricates itself from two major conflicts, China and its resurgence, organizational and crisis leadership, and the cyberspace domain. While volumes of information can be written on these topics, the following covers a subset—the nuclear ambitions of North Korea and Iran and considerations for operating in today's cyberspace domain.

Notes

[1] "Air Force Research Institute, Air Force Fellows." USAF Research Institute. n.d. Web. <http://afri.au.af.mil/aff/index.asp>

[2] Dempsey, Martin E. "Gen. Dempsey's Remarks at the World Affairs Council's Global Education Gala." 7 Mar 2013. Speech. < http://www.jcs.mil/speech.aspx?id=1759>

[3] Dwight D. Eisenhower Presidential Library and Museum. n.d. Web. <http://www.eisenhower.archives.gov/all_about_ike/quotes.html>

LESSON 2: NUKES, STILL THE GAME CHANGER IN A POST-COLD WAR ERA

The Golden Anniversary of the Cuban Missile Crisis

2012 marked the 50th anniversary of the Cuban Missile Crisis. Those shaky thirteen days in October 1962 serve to remind policy makers and military professionals just how close two nations came to a global conflagration. Fortunately, leaders in Washington and Moscow averted war with what Harvard Belfer Center's Director, Graham Allison, describes as "an imaginative combination of public deal, private ultimatum, and secret sweetener."[1] Historical documents now show that if hard diplomacy had failed the Defense Department was ready to pull the trigger on 500 bombing sorties against Cuba followed by an invasion of 90,000 troops.[2] These actions would have risked tactical nuclear attack on the landing force and subsequent nuclear exchange between the US and USSR. Instead, President Kennedy's deft handling of the crisis resulted in empowering his administration to not only avoid a world war, but also curb a global nuclear footprint through the removal of Soviet nuclear weapons from Cuba, and a short time later a removal of US missiles from Turkey.

Fast forward to today. The Cold War is behind us and fewer countries possess nuclear weapons than those in the 1960s might have forecasted. In 1963, President Kennedy predicted that 15-20 states would have nuclear weapons by the 1970s.[3] Today, while an estimated 50 countries possess the technology and capability to pursue nuclear weapons, there are only nine widely considered nuclear weapons states.[4] Further, the United States and Russia have agreed to reduce the number of deployed strategic warheads (in terms of singular RVs and bombers) to 1,550 each by 2018 under the 2010 New START Treaty. The UK and France have been

reducing their arsenals from Cold War levels. China nuclear inventory remains steady, but India and Pakistan are believed to be building up their weapon stockpiles.[5] However, the countries garnering the most international attention in 2012-2013 were North Korea and Iran. The following paragraphs capture the concerns and policy implications of two of the world's pressing nuclear challenges with an unpredictable, bellicose North Korea and suspicious, opaque Iran—both in regions of critical strategic importance to the United States and its allies.

North Korea: The Precarious Nuclear Actor

The 2012 and 2013 academic year covered a period of unprecedented North Korean rhetoric and provocative actions that grew from status-quo irrationality to belligerent absurdity. North Korea took many opportunities to demand attention as a duplicitous, yet credible nuclear threat and potential proliferator of nuclear technologies and material.

Since signing on to the Treaty on the Non-Proliferation of Nuclear Weapons (a.k.a, the NPT) in 1985 (and later withdrawing in 2003), North Korea has rebuffed its stronger neighbors and the international community by successfully developing and possessing nuclear weapons. It likely has less than a half-dozen plutonium-based nuclear weapons, and is focusing its attention on expanding its long-range ballistic missile delivery capabilities.[6]

North's Korea's first nuclear test in 2006 surprised those who thought the isolated regime had neither the technical capability, nor gall, to repudiate the international community and irrevocably risk its own survival. Fast forward to 2012/2013. Two months after a successful rocket launch that placed an object into orbit and bolstered an indigenous ballistic missile program, North Korea's nuclear test on February 12, 2013 communicated to the world that it remains undeterred in advancing its nuclear ambitions. On the surface, decades of international

isolation have seemingly empowered Kim Il-sung's family lineage with a young Kim Jong-un upping all previous antes—at least on a rhetorical front.

North Korea modified its constitution in 2012 declaring itself a nuclear power.[7] Furthermore, Kim Jong-un affirmed in his first public speech in 2012 that his "first, second, and third" priorities were to strengthen the military. In the same speech he celebrated a new era where foreign powers could no longer intimidate North Korea with atomic weapons. As North Korea readied itself for its third nuclear test in February, it clearly asserted its aspirations by "not disguising the fact that the various satellites and long-range rockets we will fire and the high-level nuclear test we will proceed with, are aimed at our arch enemy, the United States."[8] With a successful multi-stage rocket launch and nuclear test to his name, it appears the 30-year old Kim Jong-un is growing confident in his power consolidation. While North Korea's blunt threats to launch nuclear strikes against the United States are considered by defense experts and diplomats as hubris, its capability to jeopardize the economies and people of South Korea and Japan is real, not to mention threaten the thousands of US forces stationed within those two nations.

Security implications are indeed obvious in the Pacific, a critical node for economic globalization and a region replete with US interests that span the entire Pacific Command area of responsibility. As such, President Obama asserted in his 2013 State of the Union address that the United States will stand by its allies, bolster missile defense, and take the lead in containing the North Korean threat.[9] As the United States rebalances its strategic focus to the Pacific, North Korea will demand a fair amount of attention as each element of national power is employed and juxtaposed against the cooperative, competitive environment the United States and China shares. The following Diplomacy, Information, Military, and Economic (DIME) elements apply to the North Korean situation.

Diplomacy. Unlike the conduits in place during the Cuban Missile Crisis, no real diplomatic engines exist between the United States and North Korea. Recent diplomatic moves from North Korea are trending in the wrong direction with its national press again declaring "the United States has reduced the [60 year] armistice agreement to a dead paper" followed by reported actions of the North Korean government severing the phone line between the two Koreas put in place to reduce tensions in times of crisis.[10]

The United States' has an opportunity to leverage the international community, and China specifically, short of directly engaging Kim Jong-un. Since the days of the Korean War, China has shown to have the most credible leverage in shaping North Korea's actions, but on the surface seems unable to break from its traditional allied stance and curb the Kim regime's rhetoric and provocative actions. Scholars writing for China's nationalistic newspaper capture China's dilemma:

> The nuclear issue complicates Sino-North Korean relations, adding strategic difficulties to China in Northeast Asia. China has many misgivings when handling relations with Pyongyang, but there is a general principle: China is never afraid of Pyongyang. Pyongyang's diplomacy is characterized with toughness. But if Pyongyang gets tough with China, China should strike back hard, even at the cost of deteriorating bilateral relations.[11]

In response to the February 2013 nuclear test, China's diplomatic condemnation and support of the unanimous UN National Security Council Resolution 2094 that levies significant sanctions may provide a glimpse of its willingness to act tough with North Korea.[12] The question is will China follow through with the sanctions that severely restrict North Korea's financial assets and means of trade. This situation provides a laboratory for shrewd observers—diplomatic and military—on the true strength of China's regional power that aims to stem North Korea's collapse, which it fears could result in a unified peninsula under the United States'

patronage. How China deals in the long term with North Korea's nuclear situation, either bilaterally or within the UN National Security Council, will be a litmus test on whether US and China's interests can intersect—for if common ground cannot be found when dealing with a mutual strategic liability, then hope for cooperation in other regional security matters will be diminished.

Information. Information and diplomacy are indeed linked with the North Korea situation. North Korea displayed its mastery of blustery rhetoric and nuclear saber rattling on May 30, 2013 with its "do or die" declaration of 'war' against the United States and the Republic of Korea.[13] This was preceded by released photos of DPRK generals planning an invasion across the DMZ and against the United States' mainland. Without any significant change in the posture of North Korean forces, Kim Jong-un's declaration is filled with language befitting of an April fool's joke. Nevertheless, the recent actions and rhetoric beg the question of what Kim Jong-un is trying to gain. Is he trying to leverage entitlements/concessions from the international community as his father did? Is he wresting legitimacy and consolidating power within his regime from those who may doubt his resolve, or is he trying to embolden or distract a neglected population?

The quick succession of nuclear-related events and increasingly aggressive warlike pronouncements from North Korea alarmed its neighbors. South Korea's newly elected President Park Geun-hye gave notice a day after the 30 May 'war' declaration when she told her generals, "I consider the current North Korean threats very serious. If the North attempts any provocation against our people and country, you must respond strongly at the first contact with them without any political consideration."[14] North Korea's rhetoric has left President Park little

political maneuver space, creating tangible flash points in the midst of heightened distrust and tension.

China appears to be growing wary of North Korea's bluster as well. In response to North Korea's announcement to commence its February nuclear test, China published in its nationalistic paper, ""If North Korea engages in further nuclear tests, China will not hesitate to reduce its assistance to North Korea," but also warned if the U.S., Japan and South Korea "promote extreme U.N. sanctions on North Korea, China will resolutely stop them and force them to amend these draft resolutions."[15] Following the test in a United Nations Security Council session that lasted only three minutes, China supported UNSCR 2094 in which Susan Rice, the US Ambassador to the United Nations, described as "significantly impede[ing] North Korea's ability to develop further its illicit nuclear and ballistic missile programs, as well as its proliferation activities."[16] While the resolution targeted the assets of key research and development entities within North Korea and cracked down on banks that commit illicit transactions, the council did not draft it under Chapter 7, Article 42 where UN member countries are allowed to use air, sea, or land forces to enforce the sanctions.[17] A test of the efficacy of the restrictions will be whether North Korea will have the means to reopen its Soviet-era reactor at its Yongbyon nuclear facility and produce additional fissile material—a step it announced three days after its declaration of 'war.'[18]

<u>Military</u>. A strong United States military has been used over the past half century as the region's primary deterrent to North Korea, with South Korea and Japan flourishing under this security umbrella. In addition to the President's State of the Union Address reaffirming the United States' commitment to its allies, the United States responded to North Korea's threats with tangible displays of might. Timed with the annual Foal Eagle military engagement exercise

with ROK Forces, the Air Force sent B-52 bombers, F-22 air superiority fighters, and the always 'picture worth a thousand words' nuclear-capable B-2 stealth bomber to South Korea.[19] The unique airpower display is only the tip of the spear of the US' capability to show powerful restraint backed by a credible, formidable joint force of unmatched air and space power, ground forces, naval missile defense, surface warfare, and undersea capabilities.

As long as North Korea proclaims itself the enemy of the United States and its Asian allies, security in the region must be sustained by US conventional military forces with anti-access, area denial capabilities, a strong missile defense shield, and a sustained US nuclear deterrence. The US has a consistent challenge to balance its military posture and apply its diplomacy to effectively 1) deter North Korean aggression 2) keep China from interpreting actions and postures as hostile to their interests and 3) reassure South Korea of US resolve and the efficacy of its nuclear deterrent. Maintaining credibility of the US nuclear umbrella becomes more challenging as South Korea grows its modern defense force while continuing to fill shortfalls with US capabilities. There is a movement within members of South Korea's leadership and general population calling for a return of US tactical nuclear forces absent since 1991 or withdrawal from the NPT to pursue an indigenous nuclear capability vis–à–vis the India/Pakistan mutual deterrence model. In a March 2011 poll, prior to the most recent heightened tensions, over 69% of South Koreans expressed a desire for reintroduction of US tactical nuclear forces on the peninsula, and 72.5 percent called for an indigenous nuclear weapon capability.[20] Stemming from frustrations with diplomatic failures over two decades that led to a nuclearized North Korea, South Korea's pursuit of nuclear weapons—technology well within its abilities—would at a minimum force China and the US' hands to resolve the situation, or at a maximum result in South Korea gaining a sovereign deterrence capability.

Either way, this act would complicate the balance of power in the region, risk nuclear exchange between the two Koreas, and challenge the regional non-proliferation positions of the United States and China. Nevertheless, it's safe to say the US military will maintain a significant role in the security of northeast Asia for the long haul as the consequences of its absence or a too-thin presence would be too great to bear.

Economic. North Korea is pinned between two economic powers, China and South Korea—nations having strong interconnected economies with the United States. China is the second largest economy in the world behind the United States and South Korea has benefited from four decades of technological growth and is a member of the world's top 20 economies.[21] Per some estimates, China accounts for 70% of North Koreas trade, but North Korea accounts for only 1% of China's trade.[22] This trade imbalance places China in the most advantageous position to squeeze North Korea even further than what years of UN sanctions have, but the question remains if it will—especially if it envisions North Korean regime collapse as a consequence.

Juche

When considering elements of national power, North Korea is a catalyst in the Pacific region that tests the power of regional states—either individually or in a consolidated fashion. By ignoring the influence and authority of UN member states, Kim Jong-un appears to be reinforcing his nation's international relations philosophy of *juche* that rejects interdependence on other states.[23] *Juche* has been the official state ideology of the North Korean regime since Kim Il-sung instituted it in 1972—which he and his son, Kim Jong-il, often broke to take advantage of concessions from the international community in return of curbing threatening

actions. In English, North Korea is acting in a classic 20th century realist model, which Harvard Professor Joe Nye best defines as:

> Realism assumes that in the anarchic conditions of world politics, where there is no higher international government authority above states, they must rely on their own devices to preserve their independence, and that when push comes to shove, the ultima ratio is the use of force.[24]

It's easy to see how a self-isolated North Korea has grown to assume an anarchic role in the region. With no kinship in the world other than a reticent one with China, one might find it logical (albeit dangerous) for North Korea to reinforce itself as a credible military threat in which others might not want to trifle, but instead engage carefully and diplomatically. The question remains whether states with regional influence will leverage a combination of their own soft and hard powers to keep North Korea from creating a defense dilemma that can only be addressed through military action. In addition to obvious homeland defense concerns, the United States has a strong stake in peace and stability in East Asia, with interests in bolstering a cooperative bilateral relationship with China.[25] Will North Korea's nuclear situation be an impetus for cooperation or nagging source of tension between the United States and China?

Perhaps North Korea is watching what plays out in the nuclear saga that has been unfolding in Iran for years. Possibly muddying the waters, press reports have hinted at the possibility that North Korea might be testing nuclear capabilities for both itself and Iran.[26]

Iran: A Nuclear State in Waiting?

As with North Korea, the Iranian nuclear standoff is occurring in another fragile and complicated strategic region, and tests the patience and resolve of its neighbors and the world. In addition to the strong 'no containment' policy of the United States, the international

community rejects Iran's rise as a nuclear weapons power per six UN Security Council resolutions on the subject.[27]

Iran claims nuclear weapons are contrary to religious teachings, and that its activities at declared nuclear sites are civil in nature and necessary to augment the nation's energy resources. Yet, critics declare Iran has a guaranteed supply of nuclear fuel from Russia to operate its one commercial nuclear reactor at Bushehr. To run Bushehr for one year by itself, Iran would have to generate more than 20 times its current capacity of <5 percent low-enriched uranium (LEU), the fuel necessary to power a reactor.[28] Robert Reardon, a Research Fellow at Harvard Kennedy School's Belfer Center for Science and International Affairs and former RAND fellow, assessed:

> Iran has not demonstrated the ability to turn its [<5% LEU] into fuel assemblies suitable for the Bushehr reactor—no simple engineering feat, particularly if Russian assistance is not forthcoming. Tellingly, Iran's enrichment program is much better suited for producing weapons. At 2011 production rates, Iran could produce enough [LEU] for an additional nuclear weapon every 8-9 months. [29]

While it appears Iran is not generating enough fuel for its one nuclear reactor, it is enriching uranium further for some other intended purpose. In 2010, Iran began enriching <5 percent LEU to 20 percent at the Natanz nuclear facility, a plant with approximately 25,000 centrifuges used to further separate and enrich the fuel. Additionally, Iran's once secret and fortified enrichment plant at Fordow has been operational since 2011 and employs 2,784 centrifuges.[30] In explaining why it is enriching uranium beyond approximately 5%, Iran claims levels near 20 percent are needed for its Tehran research reactor (and other purported future reactors) with the goal of developing cancer treatment radioisotopes.[31] Another plausible explanation is that Iran is generating enough 20 percent enriched uranium to expeditiously jump to weapons-ready material when it wishes. Enriching uranium consumes more time up front, and processing material to 20% greatly reduces the timelines needed to further convert to weapons-grade material of

approximately 90% enrichment. Harvard's Graham Allison explains the scenario well with a football conceptual aid:

> A stockpile of uranium enriched at 20 percent shrinks the potential timeline for breaking out to bomb material from months to weeks. In effect, having uranium enriched at 20 percent takes Iran 90 yards along the football field to bomb-grade material. Pushing it back below 5 percent would effectively move Tehran back to the 30-yard line—much farther from the goal of bomb-grade material.[32]

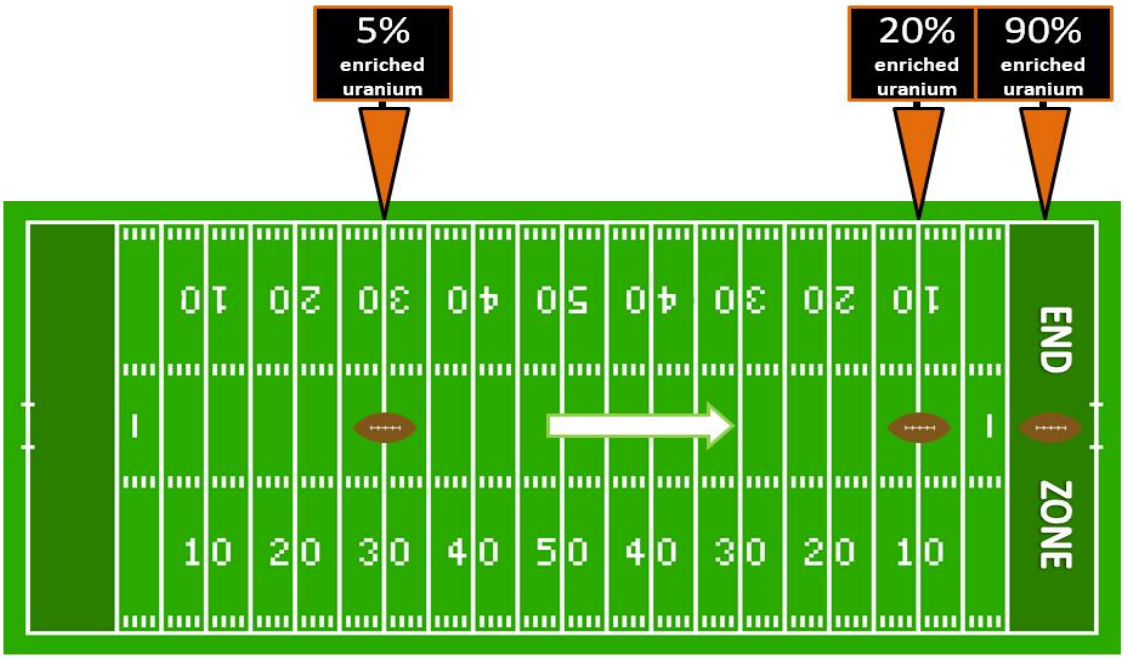

Figure 1: Illustration of Graham Allison's Explanation of Iran's Uranium Enrichment Levels in Relation to Weapons Grade Advancement

In 2010, Iran declared itself a nuclear state and President Mahmoud Ahmadinejad affirmed Iran has the capability to enrich uranium more than 20 percent, but "doesn't need to."[33] Analysts believe Iran is producing near weapons-grade uranium at a rate of approximately 10 kilograms per month, and has enough for one bomb's worth of material and is on its way to a second.[34] The big question is if Iran has the capability, or will, to 'break out' further and finalize a weapon.

In September 2012, Israel's Prime Minister Benjamin Netanyahu evoked a similar model as Allison's with a cartoon when he implored to the United Nations General Assembly that Iran is crossing its last red line by enriching enough weapons grade material and is finalizing it for a bomb.[35] In contrast, President Obama stressed there is time for a diplomatic solution and Iran is still within a year of developing a weapon.[36]

Figure 2: Israeli Prime Minister Benjamin Netanyahu's Presentation to the United Nations General Assembly on 27 September 2012
(Source: CNN.com)

Processing enough weapons grade material is only part of the equation. As for weapon fabrication and testing, the International Atomic Energy Agency (IAEA) has persistent concerns of a "possible existence in Iran of undisclosed nuclear related activities involving military related organizations, including activities related to the development of a nuclear payload for a missile."[37] Specifically, Iran appears to have built a large explosives containment vessel to conduct hydrodynamic experiments at Parchin military complex dating back to 2000. Hydrodynamic experiments study the performance of nuclear weapons assemblies via high explosive testing, and per the IAEA are "strong indicators of possible weapon development."[38]

Satellite imagery available to the IAEA depicted almost no activity near the building housing the vessel between 2005 and January 2012, but after the IAEA's request for access to the location in February 2012, the following have been observed:[39]

- Frequent activities involving equipment, trucks, and personnel
- Run off of large amounts of liquid from the containment building over a long period of time
- Removal of external pipe work from the containment vessel building
- Razing of five other nearby buildings and the site perimeter fence
- Reconfiguration of electrical and water supply infrastructure
- Shrouding of the containment vessel building and another; and,
- Digging, scraping, and filling of earth in an area covering 61 acres

The Iranian government responded to the IAEA that "the allegation of nuclear activities at the Parchin site is baseless," but has not allowed access to the site to confirm.[40] Experts question the earnest cleanup of the site, and fear the passing of each day gives Iran a chance to erase any signatures of nuclear activity at Parchin while forging permanent doubt on its former function.

The Iranian nuclear situation provides more questions than answers. For example, has Iran's regime applied observations from the situations in North Korea and Libya? (Kim Jong-un seems empowered by his country's immature nuclear weapons and Gaddafi—who decommissioned Libya's nuclear weapons program in 2003—was toppled in 2011 by his people with the help of a NATO-led force.) Is Iran using its enrichment effort as a scalable bargaining chip to tacitly bolster its own security despite heavy international suspicion? Does Iran feel that preserving nuclear weapon related technologies, material, and intellectual capital gives it the ability to hedge against security threats in the region and outweighs the consequences of pressing sanctions, international discredit, and possible military action? Monsour Salsabili, a Research Fellow at Harvard Kennedy School's Belfer Center for Science and International Affairs and former Iranian diplomat, emphasizes what scholars on both sides of the discourse have expressed:

> Despite many speculations that Iran is looking for nuclear weapons, the country is a member of the NPT and has repeatedly denied any intention of acquiring nuclear weapons. It has, however, long been involved in developing nuclear technology. Thus, if Iran decides to produce a nuclear explosive device, there is an embryonic capability to do so in a certain period of time, albeit under harsh and risky international, as well as regional, circumstances.[41]

Boiled down, Iran has the means to become a nuclear weapons power. Does it have the will, and under what circumstances does it feel compelled to execute the option? In the meantime, will its neighbor's and international community's patience wear thin? The situation is ripe for a strong diplomatic move. Early 20th Century humorist, Will Rogers, said, "Diplomats are just as essential to starting a war as soldiers are for finishing it." As President Kennedy and his leadership team showed during the Cuban Missile Crisis, diplomats are in the best position to prevent war.

As with 1962, diplomats and international security experts face a risky security dilemma with Iran. While failures in diplomacy are unlikely to rupture into instantaneous global conflict, subsequent effects of today's actions risk further destabilizing the Middle East, creating an environment where other regional states feel the need to pursue nuclear weapons, or compelling Israel to take military action against what it declares an existential threat. Unlike 1962, diplomatic conduits are not readily in place that allow potential belligerents to find mutual ground and work towards resolution. Further, the physical 'red line' drawn in the Atlantic by the 1960s US Navy to blockade Soviet ships en route to Cuba is far different than today's ambiguous nuclear processing related 'red-lines'; as a consequence, the time nations have to act is vexing and ambiguous.

Conclusion--Brief Lessons for the Military

In a global order where military power alone will not solve the world's greatest problems, one might ask where is President Kennedy's mix of diplomatic tools today for North Korea and Iran? Without clear communication conduits and transparency, is conflict inevitable? From a military perspective, President Kennedy's speech to West Point on June 6, 1962 still applies today as it did in the most dangerous years of the Cold War. Kennedy eloquently remarked:

> Above all, you will have a responsibility to deter war as well as to fight it. For the basic problems facing the world today are not susceptible of a final military solution...Our forces, therefore, must fulfill a broader role as a complement to our diplomacy, as an arm of our diplomacy, as a deterrent to our adversaries, and as a symbol to our allies of our determination to support them.[42]

Credible and executable military power is the centerpiece of the 'all options' table and its intrinsic lethality remains the United States' strongest deterrent mechanism as it underwrites the security of allies in the Middle East and Asia. Maintaining its credibility as a full-spectrum, decisive, global-reaching force backed by a robust missile defense infrastructure will be a challenge in the near-term as the United States recovers from a recession and streamlines its military after over a decade of ground-based wars. But, as history has shown after WWI, WWII, Vietnam, and the Cold War, the US military will evolve accordingly. Further, nuclear forces will continue to play a key role as a deterrent.

While the Cold War slips away from the memory of those charged with the nation and its allies' defense, nuclear weapons remain the ultimate bargaining chip played by national leaders wishing to throttle conflict or bolster peace. US military practitioners play a key role in assuring deterrence by maintaining a safe, highly professional, and extraordinarily credible nuclear enterprise and recognize flawless nuclear stewardship is of the utmost priority that cannot be minimized or ignored. On the other hand yesterday's Cold War nuclear triad will likely continue

to morph towards increased disarmament. The Department of Defense asserts the possibility that deterrence goals can be achieved with a smaller nuclear force.[43] Nuclear stand-offs with North Korea and Iran remind military practitioners of the potent threat of nuclear states—whether infantile or burgeoning—and the value of nuclear deterrence in the 21st Century where the question of "how much is good enough" will continue to shape the international nuclear equilibrium.

Notes

[1] Allison, Graham. "Fifty Years After Cuban Missile Crisis: Closer Than You Thought to World War III." *Christian Science Monitor*. Web. 15 Oct 2012. < http://www.csmonitor.com/Commentary/Opinion/2012/1015/50-years-after-Cuban-missile-crisis-closer-than-you-thought-to-World-War-III>
[2] Ibid.
[3] Schlesinger, Arthur M. *A Thousand Days, John F. Kennedy in the White House*. Boston: Houghton Mifflin, 1965. Print.
[4] "Nuclear Weapon and Fissile Material Stockpiles and Production (2011)." *International Panel on Fissile Materials*. Jan 2012. Web. <http://fissilematerials.org/library/gfmr11.pdf >
[5] Ibid.
[6] Ibid.
[7] Kwon, K.J. "North Korea Proclaims Itself a Nuclear State in New Constitution." *CNN*, 31 May 2012. Available at: http://www.cnn.com/2012/05/31/world/asia/north-korea-nuclear-constitution/index.html
[8] BBC News Asia. "North Korea Plans Third Nuclear Test." *British Broadcasting Company*, 24 Jan 2013. Web. <http://www.bbc.co.uk/news/world-asia-21175466>
[9] Obama, Barack H. "Remarks by the President in the State of the Union Address**."** 12 Feb 2013. Speech. <http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address>
[10] Miles, Donna, "North Korea Nullifies Armistice, Key Resolve Kicks Off." *Armed Forces Press Service*, 11 Mar 2013. Web. < http://www.defense.gov/news/newsarticle.aspx?id=119487>
[11] "China Should Not Fear NK Disputes." *Global Times*, 6 Feb 2012. Web. <http://www.globaltimes.cn/content/760434.shtml>
[12] "Security Council Strengthens Sanctions on Democratic People's Republic of Korea, in Response to 12 February Nuclear Test." UNSCR 2094. *United Nations*. 7 Mar 2013. Web. <http://www.un.org/News/Press/docs//2013/sc10934.doc.htm>
[13] Fisher, Max, "Here's North Korea's Official Declaration of 'War'." *The Washington Post*, 30 Mar 2013. Web. < http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/30/heres-north-koreas-official-declaration-of-war/>
[14] Sang-Hun, Choe, "South Korea Gives Military Leeway to Answer North." *New York Times*, 1 Apr 2013. Web. < http://www.nytimes.com/2013/04/02/world/asia/south-korea-gives-military-leeway-to-answer-north.html?pagewanted=all&_r=0>
[15] Riveria, Gloria, "North Korea's Newest Threats Irks Its Main Ally China." *ABC News*, 25 Jan 2013. Web. <http://abcnews.go.com/International/north-koreas-newest-threats-irk-main-ally-china/story?id=18310899>
[16] Cha, Victor and Kim, Ellen, "UN Security Council Passes New Resolution 2094 on North Korea." *Center for Strategic and International Studies*, 7 Mar 2013. Web. <http://csis.org/publication/un-security-council-passes-new-resolution-2094-north-korea>
[17] Ibid.
[18] The Yongbyon reactor was shuttered in 2007 as part of a diplomatic deal that resulted in increased aid to North Korea. It is designed to produce weapons-grade plutonium and was likely the contributor to material used in Pyongyang's 2006 and 2009 tests, but officials remain uncertain about the material used in the 2013 test.
[19] Strobel, Warren. "U.S. B-2 Bombers sent to Korea on Rare Mission: Diplomacy not Destruction." *Reuters*, 30 Mar 2013. Web. <http://www.reuters.com/article/2013/03/30/us-korea-north-usa-b-idUSBRE92S0IE20130330>
[20] Cheon, Seongwhun, "Should the US Consider Redeploying Tactical Nukes in South Korea?" *Global Asia*. June 2012. Web. <http://www.globalasia.org/V7N2_Summer_2012/Seongwhun_Cheon.html>
[21] "The World Factbook." *Central Intelligence Agency*. n.d. Web. <https://www.cia.gov/library/publications/the-world-factbook>
[22] Hatton, Celia. "China's Delicate Balancing Act with North Korea." Attributed to Marcus Noland, Senior Fellow and Director of studies at the Peterson Institute for International Economics. *BBC World News*, 13 Feb 2013. Web. <http://www.bbc.co.uk/news/world-asia-china-21441917>
[23] Lee, Grace., "The Political Philosophy of Juche." *Stanford Journal of East Asian Affairs*. Vol 3, No 1, Spring 2003. p. 105
[24] Joseph S. Nye, Jr. *The Future of Power*. New York: PublicAffairs, 2011. Print. p.18.
[25] "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense." *US Dept of Defense*. Jan 2012. p.2
[26] Sanger, David and Sang-Hun, Choe, "North Korea Confirms It Conducted 3rd Nuclear Test." *New York Times*, 11 Feb 2013. Web. <http://www.nytimes.com/2013/02/12/world/asia/north-korea-nuclear-test.html>

Notes

[27] UNSCRs 1696, 1737, 1747, 1803, 1835, and 1929 address Iran's nuclear program. The central demand by the council is that Iran suspend its uranium enrichment program, as well as undertake several confidence-building measures outlined in Feb 2006's International Atomic Energy Agency (IAEA) Board of Governors resolution.
[28] Reardon, Robert J. "Containing Iran: Strategies for Addressing the Iranian Nuclear Challenge." *RAND Corporation,* 2012. p. 47.
[29] Ibid.
[30] "Implementation of the NPT Safeguards Agreement and Relevant Provisions of the Security Council Resolutions in the Islamic Republic of Iran." *IAEA.* 16 Nov 2012. Paras 11-24. <http://www.iaea.org/Publications/Documents/Board/2012/gov2012-55.pdf>
[31] "Iran Will Not Halt 20% Enrichment" *Tehran Times,* 18 Dec 2012. Web.
[32] Allison, Graham, "Obama Should Test Iran's Nuclear Offer." *The Washington Post,* 6 Oct 2011. Web. <http://articles.washingtonpost.com/2011-10-06/opinions/35280722_1_uranium-enrichment-civilian-power-plants-nuclear-offer>
[33] Slackman, M Michael. "Iran Boasts of Capacity to Make Bomb Fuel." *New York Times,* 11 Feb 2010. Web. <http://www.nytimes.com/2010/02/12/world/middleeast/12iran.html>
[34] Zarif, Maseh, "The Iranian Nuclear Program: Timelines, Data, and Estimates V6.0." American Enterprise Institute. 28 Feb 2013. Web. < http://www.irantracker.org/nuclear-program/zarif-timelines-data-estimates-february-28-2013>
[35] Friedman, Uri, "Bibi's UN Speech Puts Pressure on Presidential Candidates." *Foreign Policy Magazine*, 27 Sep 2012. Web. <http://blog.foreignpolicy.com/posts/2012/09/27/bibis_un_speech_puts_pressure_on_presidential_candidates>
[36] Connor, Tracy, Jamieson, Alastair, and Johnston, Ian, ""Obama says 'there is still time' to find diplomatic solution to Iran nuke dispute; Netanyahu hints at impatience." *NBC News*, 20 Mar 2013. Web. < http://worldnews.nbcnews.com/_news/2013/03/20/17382317-obama-says-there-is-still-time-to-find-diplomatic-solution-to-iran-nuke-dispute-netanyahu-hints-at-impatience?lite>
[37] "Implementation of the NPT Safeguards Agreement and Relevant Provisions of the Security Council Resolutions in the Islamic Republic of Iran." *IAEA.* 16 Nov 2012. Para 43. <http://www.iaea.org/Publications/Documents/Board/2012/gov2012-55.pdf>
[38] "Implementation of the NPT Safeguards Agreement and Relevant Provisions of the Security Council Resolutions in the Islamic Republic of Iran." *IAEA.* 21 Feb 2013. Para 50. <http://www.iaea.org/Publications/Documents/Board/2013/gov2013-6.pdf>
[39] Ibid, Para 52.
[40] "Implementation of the NPT Safeguards Agreement and Relevant Provisions of the Security Council Resolutions in the Islamic Republic of Iran. " *IAEA.* 30 Aug 2012. Para 43. <http://www.iaea.org/Publications/Documents/Board/2012/gov2012-37.pdf>
[41] Salsabili, Mansour. "Iran and Weapons of Mass Destruction: The Military Dynamics of Nonproliferation." Discussion Paper 2013-1, *International Security Program, Belfer Center for Science and International Affairs, Harvard Kennedy School*, Mar 2013. Web. <http://belfercenter.ksg.harvard.edu/publication/22930/iran_and_weapons_of_mass_destruction.html>
[42] Kennedy, John F. "Remarks at West Point to the Graduating Class of the U.S. Military Academy." 6 Jun 1962. Speech. <http://www.jfklink.com/speeches/jfk/publicpapers/1962/jfk226_62.html>
[43] "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense." *US Dept of Defense*. Jan 2012. p.5

LESSON 3: CYBERSPACE--THE DOMAIN DEFINING 21ST CENTURY WARFARE

With the 20th Century marking the pinnacle of the industrial and nuclear ages, the early 21st Century is being defined by a networked world and the cyberspace domain upon which it runs. Cyber activity has become the modern signature of active fault lines within the international order as evidenced by suspected skirmishes between state and non-state elements of Iran, the United States, and Israel over Iran's nuclear activity; North and South Korea; China and Japan over Senkaku island disputes; China and the United States; and so on. Hardly a week goes by without the media reporting on alleged cyber exchanges between potential belligerents, and the specter of the cyber threat grows with each public and political commentary.

On February 12, 2013, President Obama signed an executive order to improve the cyber security of the nation's critical infrastructure[1], and stressed in his 2013 State of the Union Address:

> America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our *enemies* are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.[2]

A week later the US-based cyber security firm, Mandiant, released a detailed 69 page report exposing China's military cyber espionage by the People's Liberation Army General Staff Department, Unit 61398[3.] Since 2006, Mandiant has observed the unit steal data from 141 companies across 20 major industries. It traced the attacks back to Unit 61398 through multiple means that not only included computer-based signatures and activities, but by linking public job ads, location of the unit's main building, and a variety of facility modifications needed

for considerable network operations. Mandiant asserted the sophistication and volumes of attacks observed could only be carried out by a state-managed enterprise with an estimated 1,000 servers and a staff of hundreds to thousands of English-speaking linguists, open source researchers, malware authors, and industrial experts to assess the impact of the espionage.[4]

Mandiant's information corroborated suspected cyber espionage activities China has used to pursue intellectual property and trade secrets with the aim of accelerating technical advancements for a military advantage. The following figure depicts how the unit targeted industry sectors over time, many of which match industries that China has identified as strategically relevant for its growth per its latest Five Year Plan.[5]

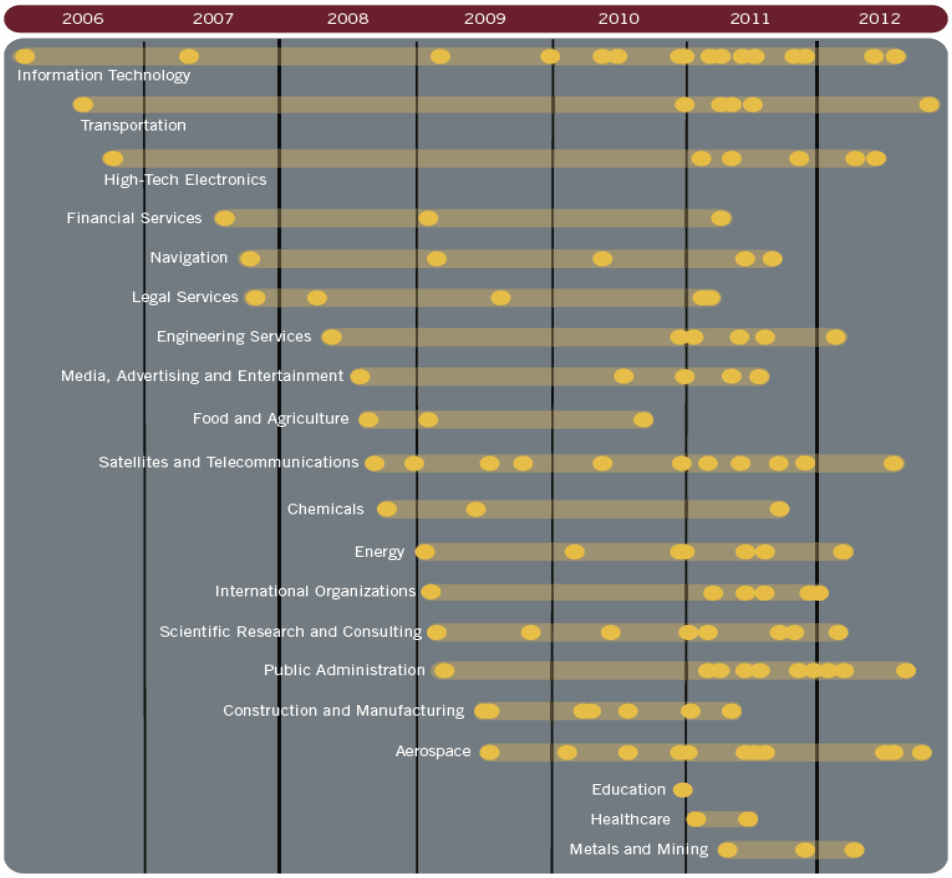

Figure 3: Chinese Unit 61398 Compromises Per Industry Sector (Source: Mandiant.com)

Other examples heighten suspicion on whether China is actively turning stolen intellectual property into weapons that match those of the United States. In June of 2012, the picture of the Chinese J-20 stealth fighter prototype's cockpit surfaced on the web exhibiting a striking resemblance to the F-22 (Figure 4).

*Figure 4: Cockpits of the Chinese J-20 and United States F-22 Fighter Aircraft (Source: China Defense Blog)*6

While Mandiant's report may not be the shot heard around the world in an escalating cyber conflict, it serves to bolster the business model of cyber security companies and does a fine job of attributing cyber espionage and intellectual property theft to China. It is also a persuasive open-source product that validates previous statements by civilian and military leaders. Admiral Samuel Locklear III, Commander of US Pacific Command, asserted to the Senate Armed Services Committee:

> China is developing organizations and capabilities that are designed to reduce the perceived technological gap. This is done by increasing China's own military technological capability, and by building capability to target U.S. military space-based assets and computer networks using network and electronic warfare. The development of these wartime capabilities is the motivation for China's efforts at peacetime penetration of U.S. government and industry computer systems. The theft of U.S. information and intellectual property is attractive as a low-cost

research and development tool for China's defense industry, and provides insight into potential U.S. vulnerabilities.[7]

Blogosphere cyber security activists and companies like Mandiant are keenly confirming the concerns of US leadership. If the United States is vulnerable to cyber activity by countries that are not declared adversaries (such as China), how prepared is it to defend itself in cyberspace in times of war? Implications for national defense in the cyberspace domain are obvious and prompt military practitioners to wrestle with the task of organizing, training, equipping, and defending a domain that is difficult to define, hard to attribute and deter within, and requires a unique type of warrior to plan and conduct effective offensive and defensive operations.

The Cyberspace Age and its Domain

The cyberspace domain that seems so common today is still a relatively new phenomenon in terms of telecommunications evolution. Samuel Morse transmitted the first telegraph message in 1844, Alexander Graham Bell placed the first phone call in 1876, the first satellite-relayed message was passed by President Eisenhower in 1958[8], and the first publically available Internet web browsers emerged in the mid-1990s.[9] Yet experts emphasize the significance of the cyber age is not how fast communications have evolved from classic point-to-point forms to a ubiquitously networked grid, but how cheap it is to transmit information.[10] Today, approximately 667 exabytes (the equivalent of nearly 7 trillion copies of an online magazine) of data flows across the Internet each year at negligible costs, all with mind-boggling growth as bandwidth, storage capacity, and computing speed increase.[11] Computers in today's society are pervasive as TVs and cell phones—with modern cell phones operating more as computers than the telephonic voice devices they supplanted. The demand and expectation of

information sharing is exploding. Between 1990 and 2005, more than 1 billion people entered the middle class and sought access to information via affordable computers and hand-held devices with ample bandwidth commensurate with their newfound status.[12]

The cyberspace domain has enabled the world to collaborate at unprecedented levels. Governments use it to manage bureaucracies, militaries to command forces, corporations to manage their workforces, inventories, and industrial secrets, banks to manage capital, etc. The cyber domain has become the equivalent of the open seas on which the world communicates and trades, and within which nefarious actors can pirate information, steal assets, disrupt communications, and recruit and train followers. Hence, cyberspace requires special attention and protection. President Obama makes specific reference to the cyber domain and calls it out separately when describing 21st century defense challenges.

> …we will continue to invest in the capabilities critical to future success, including intelligence, surveillance, and reconnaissance; counterterrorism; countering weapons of mass destruction; operating in anti-access environments; and prevailing in all domains, including cyber.[13]

Prevailing in the cyber domain, a domain that cross-cuts all others (e.g., land, air, sea, space) is indeed a challenge, especially since the cost for adversaries to access it is so low and the opportunity of asymmetric advantage so high. Furthermore, operations within the virtual domain of cyberspace are markedly different than those in classic domains. The characteristics in Table 1 are far from inclusive, but are significant factors of the cyber operating environment that require a different set of policies and Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities (DOTMLPF) elements than those typically applied to other war fighting mediums.

Operations within Classic Domains (Air, Land, Sea, Space)	Operations within Cyberspace Domain
Traditional weapons are relatively costly, and inherently inoperable amongst belligerents	Primary operating means (computers and network equipment) are prevalent and cheap—belligerents utilize similar COTS hardware/software and standards
Westphalian principles of national boundaries and sovereignty matter	Effects are not constrained within national boundaries
Laws, policies, and doctrine related to conflict are relatively mature	Laws, policies, and doctrine are underdeveloped and often contradictory. Ambiguity limits 'speed of need' operations.
Clausewitz' concepts of defense as stronger form of waging war (e.g., 3:1 rule)[14]	Over time, offense beats defense regardless of disproportionate capabilities
Time and distance are key limiting factors	Time and distance are negligible and often irrelevant
Operations are mostly overt and lethal with special care applied to make them covert	Operations are typically virtual, inherently covert, non-lethal, and reversible
Weapons effects are relatively predictable and measurable	Effects are harder to measure and 2nd, 3rd order effects are difficult to predict
Exploitation (intelligence) and attack often achieved via different means	Similar processes and assets used for exploitation and attack
Determining a target's location is first step of kill-chain	Location largely irrelevant—target specifics are characterized by bits/bytes
Actions are often attributable with burden of proof for anomalies placed on the offender	Attribution is easily masked, is hard, and never certain—burden of proof is placed on defender

Table 1: Broad Comparison of Operations within Classic and Cyberspace Domains[15]

Cyberspace and the Principles of Joint Operations

While cyber operations are distinct from those in classic domains, the principles of joint operations apply, but with key distinctions as well. Joint Publication 3-0 defines the principles of joint operations as those formed around the long-standing Principles of War with three elements added—restraint, perseverance, and legitimacy. The additional elements were codified as a result of experiences gained during recent years of irregular warfare. Air Force cyber space operations doctrine relates the Principles of Joint Operations as defined by joint doctrine.[16] The following expands Air Force doctrine and builds upon Table 1 to provide additional considerations on the unique nature of cyberspace operations.

Objective. The military purpose of specifying an objective is to "direct every military operation toward a clearly defined, decisive, and achievable goal."[17] Decisive cyber operations can be integrated across all military phases to achieve military objectives. To be effective, planners/operators must be creative and overcome the challenges of integrating virtual cyber effects with other combat capabilities.

Mass. The purpose of mass is to "concentrate the effects of combat power at the most advantageous time and place to produce decisive results."[18] To be effective, cyber operations must be synchronized to achieve mass within a short period of time. Operations within the cyber domain enable the massing effects of combat power. Additionally, massing cyber capabilities and other non-kinetic means may give numerically inferior forces an asymmetric advantage early in an armed conflict. For example, the concept of mass within cyberspace underpins Chinese PLA doctrine of fighting and winning "local wars under conditions of informatization."[19] Individuals joining the fight only need a computer, network connection, target, and synchronized method for order dissemination. With 450 million Internet users and over 675 million Internet devices[20], China could mobilize a subset of its population and employ patriotic "cyber militia" en masse to secure and dominate information while gaining a decisive military advantage over an adversary.

Offensive. The purpose of offensive operations is to "seize, retain, and exploit the initiative"[21] to enable freedom of action and decisive results in applicable warfighting domains. Operations in cyberspace favor the offense. Malware of only 100s of lines of code can penetrate and exploit one critical 'zero-day' vulnerability in security software consisting of millions of lines of code. On the other hand, precise offensive effects require extensive nodal planning,

intelligence, and timing to be decisive. Exploiting a zero-day vulnerability one moment might be easily thwarted the next with a defender simply installing a software patch.

What makes an attack difficult to attribute to an offender is what makes cyber attack attractive to the offense. In January 2013, a table-top cyber exercise was convened with a class of Harvard graduate students comprised of experts with military, international security, technology, and law backgrounds. The scenario included malware attacks against US financial markets originating from Asia with China as a prime suspect. Attributing the attacks to the state of China, or its non-state cyber militia, was difficult and created instantaneous dilemmas for students playing roles within the White House, Department of State, Department of Defense, and industry. Players concluded any response in kind from the US against China was too risky without confidence in attribution, would be easily attributable to the US, and ultimately risk escalation. It was clear that the offensive actors had the initial advantage and were allowed to maneuver accordingly while those representing the elements of US national power grappled with an effective response.

Maneuver. The purpose of maneuver is to "place the enemy in a disadvantageous position through the flexible application of combat power."[22] The maneuver of data and information is indeed applicable within cyberspace, and effective maneuver characterizes a victor.

Non-kinetic maneuver used to occupy and control segments of the electromagnetic spectrum gives forces a decisive edge during electronic warfare. Likewise, maneuver within the cyber domain between two belligerents is the process of retaining positional advantage to keep adversaries off balance, while protecting friendly freedom of action. The difficulty of cyber maneuver lies within the inherent complexity of the cyber battle space, of which can be

demarked by the theoretical layers of the Open Systems Interconnection (OSI) model, often described as the "7 layers of the Internet."[23] Table 2 depicts each layer's characteristic, whether physical (e.g., within hardware) or virtual as Merriam-Webster defines as "being on or simulated on a computer or computer network."

Layer	Description	Maneuver Realm
Physical	Physical connections (computers, cabling, networking equipment), and associated voltages	Physical
Data	Systems that make up a network and facilitate data transmission within (e.g., hubs and switches)	Physical
Network	Direct physical flow of data, i.e., as in functions performed by routers	Physical/Virtual
Transport	Data in form of bits and bytes is prepared and addressed to respective destinations within the network	Virtual
Session	Connection between both sender and destination once the physical and digital paths are confirmed	Virtual
Presentation	Syntax of data is chosen to allow its transmission and described how it will be interpreted by the receiver	Virtual
Application	Layer within which a user interacts, i.e., an e-mail client or web browser	Virtual

Table 2: Maneuver Realm for Each Layer within the Open Systems Interconnection Model

Maneuvering within the physical realm of cyberspace has tangible limits, and is restricted by physical defense measures. For example, the U.S. military's ban of thumb drives on Department of Defense networks is one way of actively defending networks from physical intrusion. Exploiting or defending underwater cabling is another way of controlling the physical cyber realm. Software firewalls are examples of virtual defenses. In an effort to maneuver and gain an advantage, opposing forces can and will find ways to exploit static defenses—whether physical or virtual.

Economy of Force. The purpose of economy of force is to "expend the minimum essential combat power on secondary efforts in order to allocate maximum power on primary efforts."[24] Economy of force involves deliberate and measured allocation of power to tasks such as limited attacks, delays, deception, etc. Cyberspace operations are the ultimate economy of force tool. In a non-kinetic, reversible fashion, they can be used as force multipliers in support of tactical, operational, and strategic tasks in any phase of joint operations. The use of cyberspace attack on key adversary nodes can be allocated and synchronized to free kinetic assets for other purposes. For example, suspected Russian denial of service attacks on Georgian websites during initial waves of the Russia-Georgia War of 2008 aimed to cripple Georgian information services and create confusion during a synchronized ground invasion.

Unity of Command. The purpose of unity of command is to ensure "unity of effort under one responsible commander"[25] with the requisite authority to direct all necessary forces in pursuit of a common purpose. Unity of command is critical for effective cyberspace operations, especially when considering synchronization of timing, tempo, and effects with other operations. This requires figuring out who's in charge, crafting supported/supporting commander relationships for unity and common purpose, and *writing down the agreements* before operating together.

Many cyber forces are not expeditionary in nature, but are instrumental in supporting combatant commanders across the globe. Cyber elements are often characterized by combined teams of military, civilian, and contractor personnel with complex equipment and infrastructure to access the global information grid from fixed locations. The challenge is to ensure garrison-based forces can support and synchronize actions with combatant commander missions without a virtual presence being perceived as actual absence. Options to enable forces to practice unity of

command with a common purpose must be people centric, whether placing cyber liaison elements within supported commander structures, leveraging global telecommunications, and ensuring constant communication between supported/supporting commanders and their key planners.

Security. The purpose of security is to "prevent the enemy from acquiring an unexpected advantage."[26] Security in cyberspace is provided by a defense in depth process that educates users on smart cyber practices and information protection, defending portions of the cyber domain relevant to military operations (e.g., instituting firewalls around relevant military networks), and employing systems and procedures for resilient capabilities that can withstand and operate in degraded environments. The potency of an adversary attack can be reduced by making it difficult to penetrate networks and identifying and isolating affected cyber elements, but pose challenges when undetected malicious code may be resident on an affected network for extended periods of time.[27]

Perhaps the most ominous challenge to security is the procurement of information and communications technology hardware with embedded viruses and malicious back doors—essentially equipment with 'zero-day' threats built in. Some technologists joke that COTS stands for "Chinese off the Shelf" and inherently distrust telecommunications hardware manufactured in China for fears of built-in vulnerabilities. That concern may be valid. An October 2012 report by the United States House Permanent Select Committee on Intelligence to Congress warned of unintended security threats from Chinese telecommunications giants, Huawei and ZTE:

> The threat posed to U.S. national security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given the country's reliance on interdependent critical infrastructure systems; the range of threats

> these systems face; the rise in cyber espionage; and the growing dependence all consumers have on a small group of equipment providers. [28]

To overcome vulnerabilities within a cyberspace infrastructure, multiple hardware/software and specialized processes are needed to provide a layered defense against potential security threats. Furthermore, effective security measures are only effective when employed by cyber professionals who are trained with a culture of linking anomalous indications to nefarious activity and can respond appropriately to limit damage.

Surprise. The purpose of surprise is to "strike at a time or place or in a manner for which the enemy is unprepared."[29] The cyber domain accommodates silent espionage followed by surprise attacks that can produce strategic to tactical results. Former Secretary of Defense, Leon E. Panetta, warned of a surprise cyber attack when he compared modern threats to the Japanese attack on the Pacific Fleet in 1941:

> The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a "cyber Pearl Harbor:" an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.[30]

While scholars and technologists argue that non-kinetic cyber attacks alone will unlikely create a Pearl Harbor scenario, it is more probable that future scenarios could resemble a 'Cyber Benghazi' where a general threat exists, warnings are ambiguous, and a significant event results in a stunned nation with damaged confidence in security.[31] The risks are obvious in an era where confidence is a powerful intangible that drives national security, politics, and economics.

The characteristic that bolsters surprise in the cyber domain is the difficulty of determining attribution. Operations in cyberspace are inherently anonymous, multi-nodal, and

are difficult to trace for counter actions. Attributing an attack to a particular computer, thereby a potential user, was easier when computers were relatively immobile with fixed Internet Protocol addresses. In an era of Botnets and mobile devices operating on dynamic host configuration protocols (DHCPs), belligerent users can benefit from ambiguous attribution. Tracing an attack back to an IP address in one country does not substantiate that a person in that country was behind the attack, much less the government itself. As shown in the Mandiant case, attribution requires more than determining an originating IP address, but multi-source intelligence that takes significant time to gather and piece together intent.

Simplicity. The purpose of simplicity is to "increase the probably that plans and operations will be executed as intended by preparing clear, uncomplicated plans and concise orders."[32] While 'simple' is not a word used often to describe the cyber domain, effective operations are buttressed by plans and procedures that are unambiguous and consider second and third order effects, clearly define command and control hierarchies, and generate timely effects that account for limits of law, policy, and rules of engagement.

Jim Waldo, Professor of Computer Science at Harvard University's School of Engineering and Applied Sciences, further stresses, "It is important to have very clear rules of engagement for defense against a cyber attack. In fact, if you want to have any chance to respond, then the rules of engagement need to be so clear that they can be codified in a program that can be run by a computer—so that the response can be at the same speed as the attack." He also emphasizes the challenges of creating simple, well understood scripts in situations where human in-the-loop judgment would slow and impact effective response during attacks.

Perseverance. The purpose of perseverance is to "ensure the commitment necessary to attain a national strategic end state."[33] Persevering in the ubiquitous cyber domain is essential

during all phases of conflict and requires assured systems and processes. While the Internet was developed with perseverance as part of its inherent design, tangible resilience requires operating redundant capabilities that prioritize communications for planning, operations, order dissemination, intelligence, indications and warning, and assessment.

Restraint. The purpose of restraint is to "prevent the unnecessary use of force."[34] Choosing reversible cyber actions over kinetic strikes during military operations is one form of restraint. During moments of conflict other than war, cyber restraint is characterized by judicious use that does not cause significant military and political consequences. Assessing tactical to strategic effects of cyber actions are critical for crafting rules of engagement that assist forces in applying effective restraint. Predicting cascading effects of cyber actions is based on other elements in the operating environment within a strategic context. Herb Lin, Chief Scientist for the Computer Science and Telecommunications Board, National Research Council of the National Academies, compares effects in the cyber domain to those in others:

> …an essential difference between cyber attack the use of a nuclear, chemical, biological, or space weapon is readily apparent—the initial use of any nuclear, chemical, biological, or space weapon, regardless of how it is used, would constitute an escalation of a conflict under almost any circumstances. By contrast, whether a given cyber attack, or conventional kinetic attack for that matter, would be regarded as escalation depends on the nature of the operation—the nature of the target(s), their geographical locations, or their strategic significance.[35]

Legitimacy. The purpose of legitimacy is to "maintain legal and moral authority in the conduct of operations."[36] Applying international law and laws of armed conflict that were drafted for more defined domains presents a challenge in the cyber domain. Complicating matters is the inherent dual civilian/military use of cyberspace, various means for plausible deniability and difficulty of attribution, and a borderless domain in which bits/bytes bear no flag,

nor wear a uniform. Nevertheless, existing international laws and laws of armed conflict that pertain to going to war (*jus ad bellum*) and conducting war (*jus in bellow*) apply. At an interagency legal conference at US Cyber Command, Harold Hongju Koh, former Legal Advisor to the US Department of State, summarized how *Jus in bellow* principles of distinction and proportionality relate to attacks on legitimate military targets and prohibit those with indiscriminate effects "that may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated."[37] Additionally, compliance with international law bolsters US' national interests in cyberspace, and "is part and parcel of our broader smart power approach to international law as part of US foreign policy."[38]

In the absence of international standards, moral legitimacy in cyberspace is difficult to define and is affected by technical knowhow, culture, and perceptions of the art of war. For example, those who misunderstand the domain may erroneously fear doomsday-level consequences and are less likely to see military cyber actions worth the risk. Some commanders may consider operations in cyberspace too complicated and restrictive, and will opt for 'simpler' means of attack, no matter how lethal or physically destructive. Others might view cyber capabilities as anything but a weapon, and discount their effects on lives and property. Some might perceive cyber espionage as simple intelligence gathering without risk of escalation. As in all conflicts, military practitioners must apply sound judgment amidst legal obscurity and bias, and draft rules of engagement that sustain legitimacy in the pursuit of accomplishing military objectives.

The People Element

Good leaders will recognize that operating in the cyber domain is indeed less analogous to operations in the other classical domains and requires innovation in leadership, organization, management, and communication. Those who harness the cyber domain will need the ability to network at all levels—from the youngest troop to the most senior leaders. General James Cartwright, former commander of US Strategic Command, was an early adopter of networked military collaborative communications. In 2005, he drove the development of the Strategic Knowledge Integration Web, a.k.a., SKI Web, an online tool used across the force for interactive information sharing.[39] This application allowed the youngest member to input information on the same networks, in real-time, that were monitored by the most senior decision makers. To specifically bolster cyber defense, one could easily envision similar collaborative efforts and tools employed by a community of cyber warfighters to share information across military elements with interfaces to key industrial partners.

To effectively integrate cyberspace within joint operations, the military is actively shaping a cyberspace culture and team that will define the next generation of warfighters. These professionals must grapple with conflict characterized by ill-defined actors using cheap, abundant, pervasive capabilities that can deny, degrade, disrupt, deceive, and possibly damage a friendly force's warfighting ability. To be effective, these warriors must intuitively sift through virtual fogs of war, and agilely operate, while defending systems needed for mission accomplishment. The best cyber warfighters will hone tactics, techniques, and procedures to dominate the domain and give their organizations a decisive edge over an adversary. US Cyber Command recognizes this and is standing up a highly trained cadre of experts who can not only defend the nation from attack, but will help combatant commanders maneuver in the offensive to

regain an advantage. In March 2013, General Keith Alexander, Commander of USCYBERCOM and Director of the National Security Agency, announced to the Senate Armed Services Committee,

> These defend-the-nation teams are not defensive teams, these are offensive teams that the Defense Department would use to defend the nation if it were attacked in cyberspace…thirteen of the teams we're creating are for that mission set alone. We're also creating 27 teams that would support combatant commands and their planning process for offensive cyber capabilities.[40]

The challenge for senior military leaders is finding and growing the next generation of cyber warfighters who can agilely organize, think, and communicate at the human level commensurate with the systems in which they are controlling. Harvard's Jim Waldo states, "Humans are slow but smart, computers are fast but dumb"; the best cyber warfighters will bridge that gap through an innate understanding of the cyber domain and how it compresses and complicates the classic Observe, Orient, Decide, and Act (OODA) model applied at tactical, operational, and strategic levels.

The talent pool for those who can defend the US in cyberspace comes from the same nation that created a fertile ground for innovators that invented the Internet, made companies like Microsoft, Oracle, and Apple software power houses, and ushered in a global, big-data driven social networking culture with Google, Twitter, and Face book.

Historically, those with the unique skills to innovate in cyberspace have reserved their talents for a corporate market—whether as software entrepreneurs or corporate IT/security professionals—or have preferred to push the technical envelope in a "hacker" subculture that leverages nonconformity in the physical world. Some military leaders are willing to tap civilian cyber markets and recruit from them. In a speech to thousands at the annual Def Con hackers' convention, General Alexander donned a hacker's uniform of jeans and a T-shirt and stressed

common ground between his organization and the attendees.[41] In a prepared statement he emphasized:

> Global society needs the best and brightest to help secure our most valued resources in cyberspace: our intellectual property, our critical infrastructure and our privacy. The hacker community and USG cyber community share some core values: we both see the Internet as an immensely positive force; we both believe information increases in value by sharing; we both respect protection of privacy and civil liberties; we both believe in the need for oversight that fosters innovation, doesn't pick winners and losers, and retains freedom and flexibility; we both oppose malicious and criminal behavior. We should build on this common ground because we have a shared responsibility to secure cyberspace.[42]

Efforts of US military leaders to cast a wide net to attract those who would defend us in cyberspace are indeed commendable and promising. As for the Air Force, it has a rich history of embracing new operating domains and enticing volunteers with innovative, entrepreneur-like tendencies. Just as the early Airmen in the US Army Air Corps learned how to think and fight with airpower that defined warfare in the 20th Century, a new breed of cyber warfighters will share similar opportunities and challenges in the early 21st Century. However, nuances are important. Dr. Kamal Jabbour, Air Force Senior Scientist for Information Assurance, remarked, "The success of the strategic bombardment RMA in World War II depended on a technology-enabled, industry-driven superiority. In contrast, the success of cyber warfare as an RMA depends on an education-enabled technology-driven framework."[43] The President's "Educate to Innovate" campaign to bolster Science, Technology, Engineering, and Mathematics (STEM) skills of K-12 students, the Air Force Association's Cyber Patriot national high school cyber defense competitions, and annual National Collegiate Cyber Defense Competitions represent opportunities to attract and grow the human "seed corn" needed to effectively defend the cyber

domain. Targeted "express" college scholarships for those entering computer engineering and science programs are also means to recruit, educate, and grow an officer corps of cyber experts.

Regardless of the means to attract the talent that will become the nexus of a future cyber force, the investments made today will pay off over the next two to three decades—a time of projected explosive growth in cyberspace. It will be an exciting time for those who define and shape the future accordingly.

Conclusion

Cyberspace is changing the way nations defend themselves, deter adversaries, and ultimately fight. Cyberspace operations are defining the latest revolution in military affairs and are changing the way forces conceptualize operations, organize themselves, and apply technologies to enhance joint warfare. But, as with any prior RMA in history, cyberspace technologies require effective use, control, and restraint by those who understand inherent capabilities, limitations, and tactical-to-strategic effects. Zbigniew Brzezinski, National Security Advisor to President Jimmy Carter, outlines the challenges ahead in cyberspace and provides some parting advice as military practitioners shape the future:

> Calm and determined deterrence—including intensified efforts credibly to identify perpetrators as well as readiness in effect to retaliate in kind—must be the point of departure for new and genuinely reciprocal rules of the game. The need for such rules is becoming urgent.[44]

Defining those new rules is indeed the challenge and opportunity for those who will shape the future of cyberspace and define its role in 21st Century warfare.

Notes

[1] "Improving Critical Infrastructure Cyber Security." *The White House*. 12 Feb 2013. Executive Order. <http://www.whitehouse.gove/thre-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
[2] Obama, Barack H. "Remarks by the President in the State of the Union Address**."** 12 Feb 2013. Speech. <http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address>
[3] "APT1, Exposing One of China's Cyber Espionage Units." *Mandiant Corporation*. Feb 2013. Report. Available at www.mandiant.com
[4] Ibid.
[5] Ibid.
[6] "Photo of the day: J-20 2002's head up display."*China Defense Blog*. 31 May 2012. Web. <http://china-defense.blogspot.com/2012/05/photo-of-day-j-20-2002s-head-up-display.html>
[7] Advance Policy Questions for Admiral Samuel J. Locklear III, U.S. Navy, Nominee to be Commander, U.S. Pacific Command. *Senate Armed Services Committee*. 9 Feb 2012. <http://www.armed-services.senate.gov/statemnt/2012/02%20February/Locklear%2002-09-12.pdf>
[8] As transmitted across the Project Score satellite, the first artificial communications satellite. Source: "Project Score." *USAF*. n.d. Web. < http://www.af.mil/information/heritage/spotlight.asp?id=123235015>
[9] The first web browser, Worldwideweb, was invented by Sir Tim Berners Lee in 1990. Marc Andreeseen's 1993 Mosaic (later Netscape) browser allowed the average person to access the web and sparked the Internet boom of the 1990s.
[10] Joseph S. Nye, Jr. *The Future of Power*. New York: PublicAffairs, 2011. Print. p.114.
[11] "Managing Information." *The Economist*, 25 Feb 2010. Web.
[12] Ibid.
[13] "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense." *US Dept of Defense*. Jan 2012. p.5
[14] Classic military theory describes that all things being equal, the 3:1 rule of combat surmises that for an attacker to win a battle, it must have at least three times the number of forces than the defender. "Force multiplying" factors such as better training, better technology, firepower, keener intelligence, and asymmetric means (e.g., airpower against ground forces) influence this rule of thumb.
[15] Derived from multiple sources with substantive inputs by the author and from information presented at Harvard by Herb Lin, Chief Scientist for the Computer Science and Telecommunications Board, National Research Council of the National Academies
[16] "Air Force Doctrine Document 3-12, Cyberspace Operations." *USAF*. 15 Jul 2010, p. 16.
[17] "Joint Publication 3-0, Joint Operations." *CJCS*. 11 Aug 2011. App A-1.
[18] Ibid, p. A-2.
[19]"Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012." *Office of the Secretary of Defense*. 2012. p. iv. <http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf>
[20]"2012 Report to Congress" *US-China Economic and Security Review Commission.* Nov 2012. <http://www.uscc.gov>
[21] Ibid.
[22] "Joint Publication 3-0, Joint Operations." *CJCS*. 11 Aug 2011. App A. p. A-2.
[23] The OSI model was developed in 1978 by the International Organization for Standardization. Per *OSImodel.org*, "It consists of seven generic vertically stacked theoretic layers each providing data transmission functionality to the layer above or below. Each layer contains a set of systems, standards, or protocols that communicate with corresponding entities in higher layers. As each successive layer depends on the one below, data cannot jump or skip layers."
[24] "Joint Publication 3-0, Joint Operations." *CJCS*. 11 Aug 2011. App A. p. A-2.
[25] Ibid, p. A-2.
[26] Ibid, p. A-3.
[27] Clark, David D. and Landau, Susan, "Untangling Attribution." *President and Fellows of Harvard College*, 16 Mar 2011, p. 7. <http://harvardnsj.org/2011/03/untangling-attribution-2>
[28] Chairman Mike Rogers and Ranking Member C.A.Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE". *U.S. House of Representatives Permanent Select Committee on Intelligence*, 8 Oct 2012.
[29] "Joint Publication 3-0, Joint Operations." *CJCS*. 11 Aug 2011. App A. p. A-3.

Notes

[30] Panetta, Leon A. "Defending the Nation from Cyber Attack." 11 Oct 2012. Speech. <http://www.defense.gov/speeches/speech.aspx?speechid=1728>
[31] The American embassy in Benghazi, Libya was attacked on Sept 11, 2012 by a heavily armed terrorist group leaving four Americans killed and ten injured. The highly-politicized aftermath questioned how Foreign Service workers could be so vulnerable to attack and diminished national confidence in diplomat security.
[32] "Joint Publication 3-0, Joint Operations." *CJCS*. 11 Aug 2011. App A. p. A-3.
[33] "Joint Publication 3-0, Joint Operations." *CJCS*. 11 Aug 2011. App A. p. A-4.
[34] Ibid.
[35] Lin, Herbert, "Escalation Dynamics and Conflict Termination in Cyberspace." *Air University Strategic Studies Quarterly*. Vol. 6, No 3. Fall 2012. Web. <http://www.au.af.mil/au/ssq/2012/fall/lin.pdf>
[36] Ibid.
[37] Hongju Koh, Harold. "International Law in Cyberspace." 18 Sept 2012. Speech. <http://www.state.gov/s/l/releases/remarks/197924.htm>
[38] Ibid.
[39] Prakash, Alicia, "Strategic Command Bids Farewell to Cartwright." American Forces Press Service, 13 Aug 2007. Web. <http://www.defense.gov/News/NewsArticle.aspx?ID=47026>
[40] Pellerin, Cheryl, "Cybercom Builds Teams for Offense, Defense in Cyberspace." *American Forces Press Service*, 12 Mar 2013. Web. <http://www.defense.gov/news/newsarticle.aspx?id=119506>
[41] Menn, Jospeh and Finkle, Jim, "RPT-U.S. Spy Chief Asks Hackers to Help Government Secure Internet." *Reuters*, 28 Jul 2012. Web. <http://www.reuters.com/article/2012/07/28/usa-security-hackers-idUSL2E8IRE7G20120728>
[42] "Def Con 20 Speakers." *Defcon.org*. Web. 21 Mar 2013. < https://www.defcon.org/html/defcon-20/dc-20-speakers.html#Alexander>
[43] Jabbour, Kamal, T. "50 Cyber Questions Every Airman Can Answer." *Air Force Research Laboratory*, 7 May 2008, p. 7.
[44] Brzezinski, Zbigniew, "The Cyber Age Demands New Rules of War." *Financial Times*. 24 Feb 2013. Web. <http://www.ft.com/cms/s/0/170b2a62-7c5a-11e2-99f0-00144feabdc0.html#axzz2PbRB2dvi>

ACRONYMS

CDR	Commander
COTS	Commercial off the Shelf
DDOS	Distributed Denial-of-Service
DMZ	Demilitarized Zone
DOD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities
DPRK	Democratic People's Republic of Korea
IP	Internet Protocol
IT	Information Technology
OODA	Observe, Orient, Decide, Act (Model)
OSI	Open Systems Interconnection (Model)
RMA	Revolution in Military Affairs
ROK	Republic of Korea
RPA	Remotely Piloted Aircraft
START	Strategic Arms Reduction Treaty
UK	United Kingdom
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
USAF	United States Air Force
USPACOM	US Pacific Command
USSR	Union of Soviet Socialist Republics

BIBLIOGRAPHY

"Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012." *Office of the Secretary of Defense*. 2012.

"Cyber Special Edition." *Air University Strategic Studies Quarterly*, Volume 6, Number 2, Fall 2012.

"Implementation of the NPT Safeguards Agreement and Relevant Provisions of the Security Council Resolutions in the Islamic Republic of Iran. " *IAEA*. 30 Aug 2012.

"Joint Publication 3-0, Joint Operations." *CJCS*. 11 Aug 2011.

Allison, Graham and Zelikow, Philip. *Essence of Decision, Explaining the Cuban Missile Crisis*. 2nd Ed. New York: Longman, 1999. Print.

Goodman, Seymore E., and Herbert S. Lin, *Toward a Safer and More Secure Cyberspace.* Washington DC, National Research Council and National Academy of Engineering, 2007.

Ikenberry, John G. *Liberal Leviathan.* Princeton: Princeton Press, 2011. Print.

Jabbour, Kamal, T. "50 Cyber Questions Every Airman Can Answer." *Air Force Research Laboratory*, 7 May 2008.

Jabbour, Kamal, T. "50 Cyber Questions Every Airman Can Answer." *Air Force Research Laboratory*, 7 May 2008.

Joseph S. Nye, Jr. *The Future of Power*. New York: Public Affairs, 2011. Print.

Lin, Herbert, "Escalation Dynamics and Conflict Termination in Cyberspace." *Air University Strategic Studies Quarterly*. Vol. 6, No 3. Fall 2012.