REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-03-2016	Research	Jul 2015 - Mar 2016

4. TITLE AND SUBTITLE
Skynet: Revisited; A Fresh Look at Network Centric Warfare

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
David A. Cochran, Major, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC School of Advanced Warfighting
Marine Corps University
2044 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
This paper seeks to reexamine the concept of Network Centric Warfare (NCW) in the context of modern and budding technological capabilities and the contemporary strategic security landscape. Department of Defense senior leaders and decision makers can use NCW concepts to inform decisions regarding acquisitions, doctrine development, and training in order to efficiently cover the vast spectrum of potential future scenarios for military force employment. Services should invest in operational research and exercises testing the impact of diverse and numerous networks of low-fidelity sensors and sensor-shooters in a wide array of scenarios. They should also continue to invest in the resilience of information networks that are critical to optimizing the effectiveness of warfighting systems. Finally, services should pursue creative acquisitions and development methods to leverage emergent commercial technology.

15. SUBJECT TERMS
Network Centric Warfare, US Air Force, Acquisitions, Autonomy, Spectrum of Warfare

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU	27	Marine Corps University / School of Advanced Warfighting
Unclassified	Unclassified	Unclassified			19b. TELEPONE NUMBER *(Include area code)* (703) 432-5318 (Admin Office)

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at lest the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. 1F665702D1257.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234.

5d. PROJECT NUMBER. Enter al project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORS AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

United States Marine Corps
School of Advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico VA 22134

FUTURE WAR PAPER

Skynet: Revisited

A Fresh Look at Network Centric Warfare

**SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES**

AUTHOR:

David A. Cochran, Major, USAF

AY 2015-2016

Mentor: Dr. Wray Johnson

Approved: _____

Date: 01 Mar 16

DISCLAIMER:

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Introduction

Senior military leadership, policy makers, and politico-military pundits do not agree on a unified vision for the role that the US military should or will play in the next 20 years. Some argue that a rising, flexing China and an increasingly recalcitrant Russia demand that the US focus preparations on the "high-end" of war, meaning interstate conflict between major powers with modern militaries. Others point to the trends of the last 25 years, namely, continuous employment abroad in "low-end" military force missions such as peacekeeping, humanitarian assistance/disaster relief (HADR), and stability and counterinsurgency operations. Dissonance has led policy-makers to question the validity of service force structure initiatives and acquisition programs. The US Air Force (USAF) has experienced this through the highly-politicized debates over the divestiture of the A-10 and the continued funding of the F-35 program, respectively championed as mascots by low-end and high-end future war advocates.

While seemingly important for service programmers and acquisition managers, long range planners and senior leaders may not need a precise and accurate prediction of future conflict in order to successfully prepare for it. Regardless of the geopolitical landscape 20 years from now, national political leaders will desire *decision space* and will look to the military to provide *options*. Fortunately, multiple technologies are currently maturing that, if exploited, can provide these options throughout the spectrum of conflict. Exploitation, however, would require a mindset shift. The US would have to abandon its fascination with and reliance on expensive and exquisite platforms developed within a politically active defense industrial base. While some flagship programs will be needed to ensure success in the most-dangerous of potential scenarios, exponentially increasing platform development costs are unsustainable in a research and development (R&D) environment where American dominance is waning. Instead, policy makers

and defense leaders must embrace incremental technological steps using a broad systemic view of defense capability instead of focusing on generational leaps in individual platform performance.

In the late-1990s, a small group of forward-thinking senior US Navy officers advocated for large networks of less-exquisite platforms in their vision of network centric warfare (NCW).[1] While the idea may not be new, current geopolitical circumstances and fiscal constraints demand a fresh look at its potential value. Some critics of NCW observed that it demanded a peer or near-peer adversary and was therefore inefficient at the lower end of the conflict spectrum or against weak, non-state, or irregular adversaries. Emergent technologies challenge this argument and suggest the value of NCW to contribute across the range of military operations now and in the future.

This paper will seek to reexamine the idea of network centric warfare in the context of modern and budding technological capabilities and the contemporary strategic security landscape. First, it will briefly explore the conditions of this landscape and discuss the current potential demand for US military capability. From this foundation, it will explore the arguments for and against a network approach to warfare before highlighting areas for potential exploitation when posturing for military operations over the next 20 years.

The Context: Uncertainty, Relative Decline, and Fiscal Constraints

Due to the tumultuous and unpredicted security events of 2014, perhaps the most common buzzword in use today to describe the current and anticipated security environment is "uncertain." The Russian annexation of Crimea, the rapid expansion of the Islamic State in Syria and Iraq, and the Ebola outbreak in West Africa sounded a wake-up call to a US national security apparatus that had focused rather narrowly since 2001 on the counterinsurgency fights in Iraq

and Afghanistan. Although the Obama administration announced a strategic national security "pivot" to the Asia-Pacific region in 2011[2], defense officials and pundits have nevertheless been alarmed at the scale and rate of Chinese reclamation activity in the South China Sea, describing it as "dramatic" and "unprecedented."[3] Additionally, the past two years have seen an increasing appearance of successfully-executed, unanticipated cyber-attacks, attributed to both state and non-state actors against a host of commercial and governmental victims—Sony, Target, Home Depot, the US Office of Personnel Management, and the United States Central Command (USCENTCOM) to name but a few.

One could argue that uncertainty stemming from a highly complex and interconnected global system is anything but new. Indeed, scholars and security analysts have written about crafting security policy in an uncertain environment frequently throughout the post-Cold War era.[4] While unpredictability may not be a novel phenomenon, the United States' freedom of action to respond to it may be waning due to a relative decrease in national power. One can see by national gross domestic product (GDP) trend data in Figure 1 that, even though US GDP has grown every year but one this century, world GDP has grown even faster, meaning the American share of the global economy has declined while the shares represented by potential adversaries have risen.[5] Additionally, one can see by comparing absolute values of governmental spending on defense that American military fiscal dominance is in a period of change. Figure 2 shows the ratio of US defense spending to the combined defense budgets of China and Russia, a value which has declined from near thirty immediately following the Cold War to only two.[6] This is admittedly imprecise as a true comparison of military power but is useful nonetheless to highlight an undeniable trend towards defense spending parity.

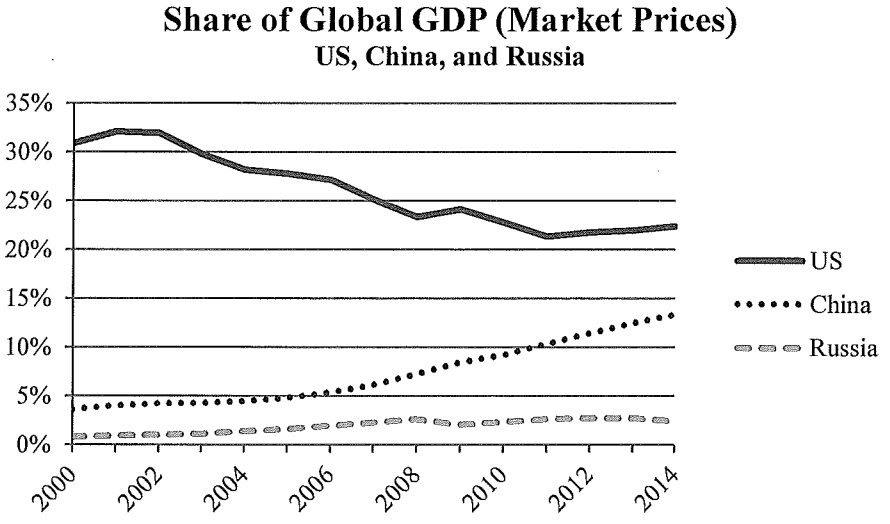

Figure 1. National GDP in Market Value of the US, China, and Russia as a percentage of global GDP.[7]

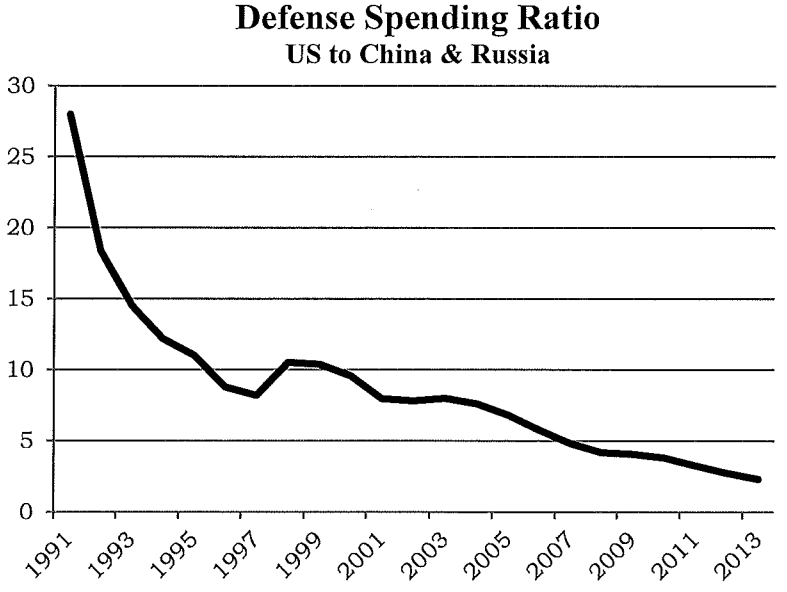

Figure 2. Ratio of Defense Spending between the US and China & Russia[8]

Amid this relative decline, American interests abroad continue to grow. Extremist networks across the Islamic Maghreb, North Africa, the Middle East, and the Afghanistan-Pakistan region threaten to export terrorism and reduce regional stability. Moreover, economic interests have increased. US foreign trade numbers (when controlled for inflation) have grown by 50% over the past 15 years.[9] As American-based multinational corporations have diversified operations globally to exploit foreign markets, more and more Americans and American interests have migrated abroad. Trade, population, and economic interdependence will likely continue as developing countries in Africa, Asia, and the Middle East, along with growing economies in South America, take on larger economic shares of the global economy. While economic interdependence has the potential to dampen interstate conflict, it also risks the creation of new arenas of competition as well as a clash of ideologies that may accompany the mixing of two previously separated cultures. US power, including military force, will likely be called upon to secure national trade interests, assure partner nations, and police the global air, space, sea, and underwater commons.

In this ever more challenging security environment, one must also consider the fiscal issues constraining national defense capacity. Partisan concerns over the treatment of the US debt ceiling have led to political gridlock, a malfunctioning budgetary approval process, government shutdowns, and across-the-board spending cuts that have crippled military readiness and inserted additional uncertainty into the defense acquisitions process. US defense spending in proportion to the economy has been fairly stable since the end of the Cold War, hovering near 4% of GDP, but in the past 5 years it has slowly but steadily declined to its lowest level since 2002.[10]

Considering present and anticipated commitments and resourcing, the US national security structure is probably best described as *stressed* at this time. Present and anticipated increases in security demands coupled with decreases in funding suggest that reform is required. The US military will continue to be called upon to execute any number of missions across a broad range of military operations—the 2015 US National Military Strategy published by the Chairman of the Joint Chiefs of Staff lists no less than twelve prioritized missions for the US armed forces.[11] How to provide these capabilities in a changing, unpredictable, fiscally-constrained environment is the principal challenge for service planners and acquisitions managers. The next section will further refine the two primary drivers of this problem: adaptability and efficiency.

The Problem: The Spectrum of Warfare and the Most Expensive Weapons System Ever

The scope and diversity of the threats discussed in the previous section dictate the need for the military forces to be ready to respond to a wide range of security demands against a range of potential adversaries. Aside from highlighting the present complexity and volatility of global geopolitics, 2014 served to reveal the incredible range of response options that may be asked of the armed forces in the interest of national, regional, or global security. Former Chairman of the Joint Chiefs of Staff General Martin Dempsey spoke in 2014 of a "two-two-two-one" framework for understanding the chief threats: two heavyweights (China and Russia), two middleweights (Iran and North Korea), two networks (violent extremists and transnational organized crime), and one domain (cyber), the importance of which is rapidly growing.[12] Dempsey's replacement, Marine Corps General Joseph Dunford, recently offered his view of the primary national security threats which, although lacking his predecessor's mnemonic, similarly contains the same diverse

list of potential adversaries and concerns.[13] Most striking from a military perspective is the unique capabilities that will be needed to counter each one.

Broadly, military policy towards China is necessarily nested within a national policy which is heavily influenced by economic interdependency and historically complicated diplomatic ties. Nuclear deterrence serves to discourage total war but conventional military competition, primarily in the air and sea domains, still exists in the East Asian commons centered on regional power balancing and assurance of third party nations who have strong connections with both major powers. For their part, Russia poses a threat owing to its proven aggression against its neighbors. While overt military conflict is again curbed by nuclear deterrence, Russia's threat is characterized by a demonstrated cyber warfare capability, non-attributable "ambiguous warfare" as seen in Georgia and eastern Ukraine, and advanced weapons proliferation to Iran, Syria, and other recalcitrant "rogue" states. Due to the scale of the impact of miscalculation vis-a-vis both "heavyweights," US military strategies necessarily must include scalable options.

Nuclear concerns certainly influence US security policy with regard to Iran and North Korea, both of which have pursued nuclear warhead and delivery technology with varying levels of success over the past two decades. American strategies on both the Korean peninsula and in the Middle East have featured theater security cooperation and providing a conventional deterrent against threatening behavior as well as assurance for regional friends and allies.

Violent extremist networks and transnational criminal organizations demand other unique approaches and capabilities. While ideologically motivated terrorism and profit driven crime are inherently different problems, both share the particular challenge of existing below the state level, limiting options for political engagement. Instead, US national policy has relied on special

operations forces targeting leadership, conventional military forces targeting capacity, and integration with law enforcement agencies at home and abroad through interagency task forces. Due to the dispersed and obscured nature of non-state organizations, wide area persistent intelligence, surveillance, and reconnaissance (ISR) and quick-reaction capabilities to apply towards time-sensitive targets have been in high demand and will likely continue to be so in the future.

Finally, cyberspace was highlighted by Generals Dempsey and Dunford as a domain of interest, one best viewed concurrently the rest of the listed primary threats. Recent incidents have demonstrated this coherence: the 2014 Sony cyber attack attributed to North Korea,[14] the 2014 indictment of five Chinese military hackers for commercial espionage,[15] and the 2015 attack on the US Central Command website by hackers claiming affiliation with the Islamic State.

So, how does the Department of Defense (DoD) optimize its organization and capability portfolios to meet the diversity of threats on the horizon? It must be prepared to gain and maintain air, space, sea, and cyber superiority and precision strike capability against a near-peer adversary like China or Russia while simultaneously performing shaping operations across the globe in support of steady-state interests and sub-state conflicts. The military must prepare for the worst by cultivating a capacity to degrade and dismantle a modern Chinese integrated anti-access/area-denial (A2/AD) system while at the same time maintaining the reach, stamina, and agility needed to support global counterterrorism efforts. The force must be *adaptable*, to provide capability across this spectrum of warfare, as well as *efficient*, to meet or exceed operational demands within tight fiscal constraints.

At the high end of the spectrum, stealth technology, integrated advanced avionics, and defensive electronic warfare packages provide an adequate counter to Soviet-era integrated air

defense system (IADS) capabilities. "Fifth generation" fighter aircraft like the F-22 Raptor and F-35 Lightning II, along with the stealthy but aging B-2 Spirit and the new B-21, now in development, provide a reasonably survivable counter-air and precision strike capability against nearly all currently-fielded adversary systems. But with the advent of counter-stealth radars, the wide proliferation of highly-maneuverable missile systems such as the S-300 and S-400, and relatively inexpensive digital control upgrades to older systems, even fifth generation platforms are becoming more and more vulnerable.[16] Could a "sixth-generation" airframe with unprecedented stealth technology, engine performance, sensors, and weapons range and accuracy regain the waning competitive edge? A brief look at the most recently-fielded fighter suggests that the extant generation-step paradigm is a losing proposition and a new sixth generation panacea platform is undeniably unaffordable and impractical.

The F-35 acquisition program, which has been widely reported as the most expensive weapons program in Department of Defense history, has by its sheer size become so politicized that a thorough and independent analysis of its need or effectiveness has become incredibly difficult. Program delays and cost overages have added significantly to an already massive development and procurement bill, pushing the overall price tag to $391.1 billion.[17] Proponents of the system focus on performance and claim its stealthiness and modern sensor suite are the keys to gaining access in areas where our adversaries are striving to prevent it. Opponents point out its spotty test record, limited payload, and unsustainable costs. Regardless of the F-35's nominal value, one thing is certain: the enormous cost of modern aircraft development is becoming unsupportable. Figure 3 shows the approximate unit cost of jet fighter aircraft since World War II plotted on a logarithmic scale. The F-22 program in the late 1990s and early 2000s was considered too costly, was significantly truncated by Department of Defense and

Congressional leadership, and then cancelled. Many are calling for a similar response regarding the F-35 program.

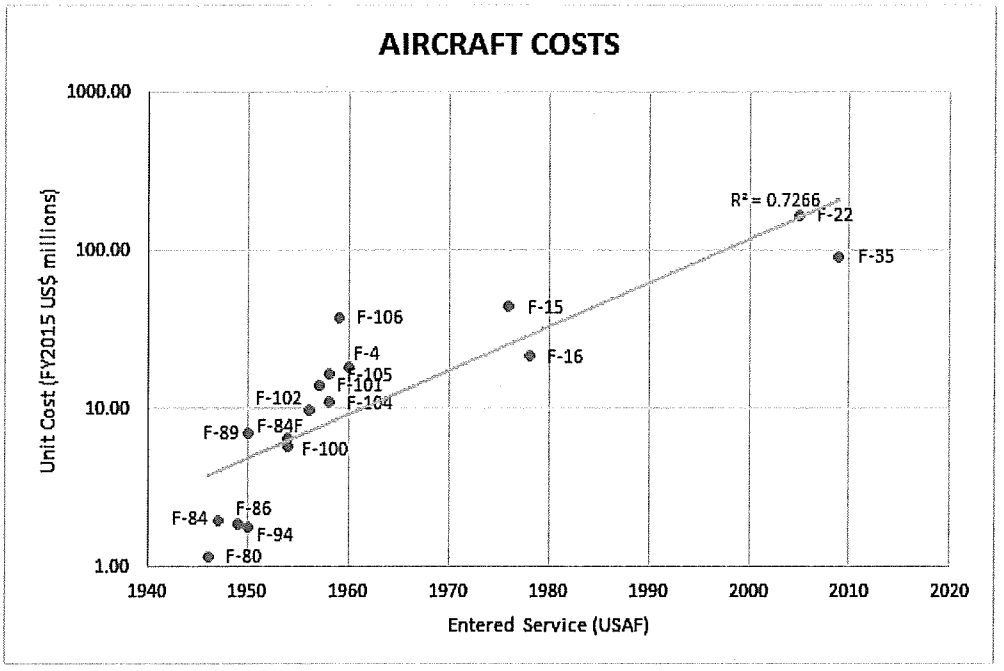

Figure 3. US Air Force Jet Fighter Aircraft Unit Costs vs. Year Entered Service[18]

In addition to startling increases in per unit cost, the aircraft development timeline has also increased in the modern era to about 15 years between the awarding of a development contract and the time when the aircraft is assessed to have reached initial operational capability. This is in stark contrast to the rapid progress in computing, communications, and electronics which have development cycles often an order of magnitude shorter. The impracticability of continuing aircraft acquisition along a seemingly exponentially-increasing cost and development time curve highlights the need to rethink the DoD's current concept of platform utility.

Instead of searching for the one platform that might provide the next great technological edge, the services must look for creative new ways to achieve desired operational effects across the spectrum of warfare, starting with dusting off an old concept.

Network Centric Warfare: Systems-of-Systems

Admiral William Owens, then-Vice Chairman of the Joint Chiefs of Staff, understood the power of network thinking well before the smart phone revolution when he wrote in 1996 about a "system-of-systems" approach to warfighting.[19] Along with a handful of other senior military officers and theorists, Owens perceived the value of a holistic view of warfighting. In a 1998 *Proceedings* article, Vice Admiral Arthur Cebrowski and John Garstka extended Owens' vision and outlined a concept of network centric warfare, a term coined by then-Chief of Naval Operations Admiral Jay Johnson.[20] "The 'power' or 'payoff' of network-centric computing," they explained, "comes from information-intensive interactions between very large numbers of heterogeneous computational nodes in the network."[21] The rapid advancement of computing power, increasing connectivity of the global community, and the explosion of information transmission rates pointed to a new age of warfare that would no longer be defined by an exchange of industrial military might but rather by the control of information. Concepts of firepower superiority were replaced with those of decision dominance.

Inspired by the extremely competitive information-centric strategies they saw being employed in the commercial sector by companies such as Wal-Mart and Deutsche Morgan Grenfell, Cebrowski and Garstka envisioned a transformation taking place in the world at large and advocated for the US to take pro-active steps to maintain military dominance by shifting to an information-based approach to warfare[22]. In their seminal 1999 volume on network centric warfare sponsored by the Command and Control Research Program, David Alberts, John Garstka, and Frederick Stein further developed the concept. They understood NCW to be a fundamental shift away from platform centric warfare.[23] The truly enabling technology for NCW, they argued, are high fidelity sensors and a network of stealthy actors that can create

effects.[24] Both of these requirements must be built upon a robust network infrastructure that facilitates communication between participants. Their ideas promoted a concept that, without significant attribution or fanfare, has created the modern concept of armed ISR. This is evident when comparing the early NCW concept with the ideas of modern theorists such as retired USAF Lieutenant General David Deptula, who has advocated for a networked sensor/shooter capability projected via a "combat cloud."[25]

Counterpoints: September 11th, Counterinsurgency, and the Politicization of NCW

The attacks of September 11, 2001, and the subsequent military operations in Iraq and Afghanistan proved to many NCW critics that the idea of a new way of warfare ushered in by the information age was misguided and incorrect. Warfare, they argued, has always been and will always be a violent clash of human wills that will be settled at a personal level and not at a system or network level. The difficult insurgencies against very low-technology threats in Iraq and Afghanistan seemed on the surface to back up this viewpoint.

However, US operations in both theaters subtly took advantage of American information superiority and cutting edge technology. MIRC, a text-based internet relay chat client used by DoD personnel, in conjunction with satellite-based communications and theater-wide datalink networks, was successful in driving the average response time for close air support (CAS) to around eight minutes in Operation ENDURING FREEDOM in 2012: that's eight minutes between a request for air support and an appropriate asset overhead *anywhere in a country roughly the size of Texas.*[26]

The most likely cause of the wane in popularity of the network centric warfare concept was not empirical evidence contradicting its premises, but rather the politicization of the expression itself and its champions. Cebrowski, after serving as the President of the Naval War

College, was offered the opportunity to lead a new Office of Force Transformation.[27] In his role as a political appointee, Cebrowski reported directly to Secretary of Defense Donald Rumsfeld and was therefore free to pursue an aggressive tack towards what he believed was the right direction for the country. In short, he believed that "only a comprehensive, integrated, innovative, and holistic strategy is likely to result in the successful transformation of an organization."[28] In response to the attacks of September 11, 2001, and the following operations in Iraq and Afghanistan, Cebrowski's fairly vague transformational concept from just three years earlier shifted to a more concrete but political "theory and strategy [that] combined Tofflerian information-age technological determinism and neorealism with concepts from nonlinear science to advocate the forceful spread of economic globalization."[29] The political tone that his advocacy took drove skeptics away. At the same time, the idea of NCW was under conceptual scrutiny from ground-centric senior leaders who were in the thick of two very personal, close-range fights in Iraq and Afghanistan and who saw NCW's technology-centric premise as out of touch with reality.

Indeed, Cebrowski and Garstka's verbiage about network centric warfare in their eponymous 1998 article gave opponents ample fodder for complaint. They promised much from the concept, noting that the intent was to achieve "lock-out" of the adversary's decision-making capability, leaving him only one rational course of action available, and likewise claimed that tactical gains enabled by network centric operations could "stop wars—which is what network centric warfare is all about."[30] On the surface these ideas contradicted more conventional views of warfare defined by a fierce and unpredictable battle of wills that were being validated in Iraq and Afghanistan. Nevertheless, the fundamental logic of the concept evaded most direct attacks. It was difficult, for example, to deny that rapid change was taking place in the commercial

sector, that situational awareness has always been and will likely continue to be aggressively pursued and coveted, and that the "co-evolution of...technology with operational concepts, doctrine, and organization" is a desirable concept.[31]

One of the more significant events that cemented the politicization of NCW was the Millennium Challenge '02 exercise during which retired Marine Corps Lieutenant General Paul Van Riper, playing the role of the adversary, successfully countered the US strategy during the wargame. When administrators waived away the impact of his decisions in the interest of continuing the exercise, Van Riper vehemently objected and complained publicly that the results of the game "were rigged to support the Pentagon's goals for force transformation."[32] Van Riper and other critics pointed to the botched test as demonstrating an inherent flaw in the DoD's attempt to automate warfare and similarly claimed that it invalidated a number of other contemporary concepts[33]. Ironically, however, the operational approach taken by Van Riper during the exercise shared many fundamental tenets with NCW. Although his forces were not connected within a robust communications network, Van Riper's strategy was holistic and sought to apply an array of capabilities against the enemy's weaknesses, allowing his own team significant leeway for decision making at the lowest levels, an idea nominally anticipated by the NCW concept of self-synchronization.[34]

As noted by Micah Zenko in a recent article about Millennium Challenge '02, "a concept-development exercise that was intended to socialize the military around the inevitability of a leap-ahead, futuristic transformation ultimately left precisely the opposite impression."[35] Essentially, it tainted the terms involved which inhibited continued development of NCW. Although some concepts have been embraced and normalized, including significant investment and reliance on ubiquitous datalinks and information networks, NCW as a buzzword and all-

encompassing transformational concept has nearly disappeared from the US military lexicon. But in light of current security challenges and maturing technologies, it may be worth another look.

Enablers: Autonomous Swarms and Facebook Drones

Events over the past two years have demonstrated that the security environment has changed, driving a reassessment of current capabilities to meet present and future challenges. Innovative thinking is required. However, this does not necessitate abandoning earlier concepts. NCW as a concept of reconciling an uncertain geopolitical landscape with accelerating information technology and global interconnectedness was born in the immediate post-Cold War period. While the priority of the US military so far this century has been to support nation-building and counterinsurgency (COIN) efforts in Iraq and Afghanistan, the social and technological undercurrents that inspired NCW remain. "The COIN fight" provided a focus that diverged from the ambiguity of the 1990s, but VUCA (volatility, uncertainty, complexity, and ambiguity), which originally surfaced in the military lexicon in the previous century, is now firmly rooted in business literature and is making a resurgence in defense circles.[36]

To some extent, the US military has quietly embraced NCW. Air, land, sea, space, and cyber operations are heavily dependent on datalinks to collect and distribute threat information, friendly force positions and postures, and to assign missions. In addition to command and control functions, network architecture and bandwidth has similarly advanced to assist weapons employment as demonstrated by the advent of net-enabled weapons and remotely-piloted "sensor-shooter" aircraft like the MQ-9 Reaper.

Advances in the field of autonomy are offering new opportunities to take advantage of the concepts merely dreamed about by the founders of NCW. Autonomous flight control systems decrease the need for human oversight of the very basic but time-consuming tasks required to

fly. While the widely-known MQ-1 Predator and MQ-9 Reaper platforms require constant input by a remote pilot, newer systems feature robust automation that allow operators to focus on less-tedious but potentially more important tasks such as sensor management, positional battlespace situational awareness, and weapons employment. In 2013, the X-47 UCAS test aircraft developed by Northrop-Grumman and funded by the US Navy was able to take off and land from an aircraft carrier and in 2015 was able to autonomously refuel.[37] These advances will pave the way for increased sortie duration, more effective human-in-the-loop oversight during mission execution, and more expeditionary placement of combat power around the globe.

The ability for autonomous entities to act in concert with one another towards a common goal truly capitalizes on the value of network warfare. Due to the speed at which computer-based decisions are made, cooperative autonomy, especially among heterogeneous entities with varying capabilities, has the potential to present a challenging problem for adversaries. A swarm executing coordinated jamming, signature management, electronic attack, and kinetic strikes is truly a systems-based operational approach to an advanced A2/AD system. In a giant stride towards this end, researchers working on the ARSENL program at the Naval Post Graduate School have achieved successful flight tests of a swarm of 50 autonomous aircraft using only two human operators.[38] Granted, the research vehicles were small hand-launched platforms, but the leader-follower cooperative behavior and vehicle-to-vehicle communication that was demonstrated will undoubtedly be realized in larger, more complicated platforms in the future.

One of the most promising candidates for such "scaling" is the Miniature Air Launched Decoy, or MALD, manufactured by Raytheon. Developed in the 1990s, MALD is an air-launched, jet-powered decoy that is able to fly 900km or loiter for 45 minutes before running out of fuel.[39] It has the ability to adjust its radar signature and "noise" profile to "look" (in the

electromagnetic spectrum) like other aircraft. Acquired in large quantities in 2009, an active jamming variant was fielded in 2012 and a datalink-enabled version was tested in 2014.[40] Although initial datalink capability will likely focus on communicating with other manned systems to provide cuing updates in flight, a future scenario is imaginable in which swarm technology pioneered in the ARSENL program could be applied to a package of networked MALDs to degrade a peer adversary's advanced IADS.

To be clear, neither this paper nor the foundational documents outlining the concepts of NCW advocate for the complete automation of warfare. Armed conflict will always be driven and controlled by human beings. However, autonomy offers new levels of human cognitive efficiency that will have significant impact on modern operational concepts of warfighting. In the Air Force's 2015 Future Operating Concept, a document projecting a vision of Air Force operations in 2035, the authors describe a force that can "operate with a balanced capability mix composed of manned, remotely operated, semiautonomous, and autonomous air, space, and cyberspace assets, including sophisticated systems to achieve adaptive domain control against advanced adversaries and lower-capability systems for actions against a reduced or less-capable array of threats."[41]

While autonomous swarms of sophisticated drones demonstrate an application of NCW at the high end of the spectrum of warfare, "lower-capability" systems are key to efficient organizational posturing against low-end threats. The commercial sector presents an emerging opportunity for efficient low-end capability acquisition. In 2015, the amount the US government spent on defense-related R&D was eclipsed by the total spent by just the top seven private global corporations.[42] Commercial off-the-shelf technology can provide incredibly potent combat-enabling power with only minor modifications. For example, high altitude internet service drones

currently being flight tested by Google and Facebook are fueled by solar energy and aim to remain aloft for up to three months.[43] With adjustments to their communications equipment and sensor payloads, these platforms could have a game-changing effect on any given battlespace, or they could even provide redundancy to many of the space capabilities on which the US military remains heavily reliant.

Conclusion

In the end we must exploit the inherent offensive and defensive potential of networks in high-end as well as low-end conflicts. With that in mind, defense leaders must look to leverage existing military and commercial technologies that can be applied to any environment, from war with a peer competitor to COIN. At the high-end, modern A2/AD systems threaten the ability of the US military to operate in a denied environment. Miniature air launched decoys (MALD), long-endurance drones, and low cost gliding or powered standoff munitions, sent *en masse*, have the potential to quickly saturate, deplete, and paralyze even the most advanced defense networks. At the low end, low-cost projectiles and airframes can be used individually in limited conflicts against minor states, sub-state organizations like terrorist networks or criminal gangs, as well as in peaceful military operations like HADR. Low-fidelity "sensor-shooter" platforms that can be purchased in large numbers with relatively cheap per-unit cost can be spread across large areas during peacetime or low-intensity conflict operations. With high levels of autonomy, secure and redundant communications links, and a common network architecture into which participants can plug and play, dispersed low-fidelity components can coalesce to form a combat network that commanders can leverage against even the most advanced potential adversaries as well as irregular opponents.

Going forward, the DoD should look to foster innovative minds within its ranks to capitalize on emergent technologies and concepts, especially with regard to the application of NCW concepts. The services should invest in operational research and exercises testing the impact of large-*n* networks of low-fidelity sensors and sensor-shooters in a wide spectrum of scenarios. They must also look to protect existing information and network advantages through investment in hardened, redundant network communications technology. Finally, it should pursue creative acquisition and development methods to leverage emerging commercial products and concepts. In conclusion, network centric warfare as an operating concept and the enabling technologies described in this essay support a cost-efficient strategy applicable across the spectrum of warfare.

---

[1] James Blaker, "Arthur K. Cebrowski: A Retrospective," *Naval War College Review*, Spring 2006, Vol 59/2, 137-138, https://www.usnwc.edu/getattachment/d1c5384c-f7fa-41b7-a6e6-490450835809/Arthur-K--Cebrowski--A-Retrospective---Blaker,-Jam.aspx.

[2] Mark E. Manyin, *Pivot to the Pacific? The Obama Administration's "Rebalancing" Toward Asia*, (Washington, DC: Congressional Research Service report, March 28, 2012), https://www.fas.org/sgp/crs/natsec/R42448.pdf.

[3] David Sanger and Rick Gladstone, "Piling Sand in a Disputed Sea, China Literally Gains Ground," *New York Times*, 8 Apr 2015, http://www.nytimes.com/2015/04/09/world/asia/new-images-show-china-literally-gaining-ground-in-south-china-sea.html.

[4] Aspen Strategy Group, *Balancing National Security Objectives in an Uncertain World (An Aspen Strategy Group Report)* (University Press of America, 1989) and Andrew F. Krepinevich, *Defense Investment Strategies in an Uncertain World* (Washington, DC: Center for Strategic and Budgetary Assessment, 2008), https://www.google.com/url?q=http://www.csbaonline.org/4Publications/PubLibrary/R.20080821.Defense_Investment/R.20080821.Defense_Investment.pdf&sa=U&ved=0ahUKEwifgMKy34PKAhUBbSYKHb7SBmsQFggFMAA&client=internal-uds-cse&usg=AFQjCNFLlLxhXpNR_ey2IwUMZ2cC_ZZBYA and J. Furman Daniel, III, "Through a Glass, Darkly: Strategic Perspective(s) for an Uncertain World," *Orbis*, Spring 2015, Vol 59/2, 287.

[5] The World Bank, "GDP at Market Prices (current US$)," The World Bank, http://data.worldbank.org/indicator/NY.GDP.MKTP.CD (accessed 30 Dec 15).

[6] Stockholm International Peace Research Institute, "SIPRI Military Expenditure Database," Stockholm International Peace Research Institute, http://www.sipri.org/research/armaments/milex/milex_database/milex_database (accessed 15 Mar 15).

[7] The World Bank, "GDP at Market Prices."

[8] SIPRI, "SIPRI Military Expenditure Database."

[9] US Census Bureau, "US Trade in Goods and Services – Balance of Payments (BOP) Basis," US Census Bureau, Economic Indicator Division, Feb 5, 2016, http://www.census.gov/foreign-trade/statistics/historical/gands.pdf.

[10] The World Bank, "Military expenditure (% of GDP)," The World Bank, http://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS (accessed 30 Dec 15).

[11] Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015: The United States Military's Contribution to National Security*, (Washington DC: The Joint Chiefs of Staff, June 2015), http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

[12] Martin E. Dempsey, "Transcript: Gen. Martin Dempsey at Disrupting Defense," The Atlantic Council, May 14, 2014, http://www.atlanticcouncil.org/news/transcripts/transcript-gen-martin-dempsey-at-disrupting-defense.

[13] Joseph F. Dunford, "Center for a New American Security/Defense One National Security Forum," Comments from the Chairman of the Joint Chiefs of Staff, Center for a New American Security, Washington, DC, 14 Dec 15.

[14] Oliver Laughlin, "FBI director stands by claim that North Korea was source of Sony cyber-attack," *The Guardian*, 7 Jan 2015, http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey.
[15] Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Department of Justice, May 19, 2014, http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
[16] Bill Sweetman, "New Radars, IRST Strengthen Self-Detection Claims," *Aviation Week and Space Technology*, Mar 16, 2015, http://aviationweek.com/technology/new-radars-irst-strengthen-stealth-detection-claims.
[17] US Department of Defense Press Operations, "Department of Defense Selected Acquisition Reports (SARs) (As of December 31, 2014)," News release no. NR-090-15, March 19, 2015, http://www.defense.gov/News/News-Releases/News-Release-View/Article/605423/department-of-defense-selected-acquisition-reports-sars-as-of-december-31-2014.
[18] James Mugg, "Jet Fighter Costs: A Complex Problem," *The Strategist*, 21 Sep 2015. http://www.aspistrategist.org.au/jet-fighter-costs-a-complex-problem/.
[19] William A. Owens,"The Emerging U.S. System-of-Systems," *Strategic Forum* 63 (February 1996). www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394313.
[20] Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare: Its Origins and Future," *Proceedings*, January 1998, http://www.kinection.com/ncoic/new_origin_future.pdf.
[21] Ibid., 3.
[22] Ibid., 1.
[23] David S. Alberts, *Network Centric Warfare*, (DoD C4ISR Cooperative Research Program, Feb 2000), 2.
[24] Ibid., 68.
[25] David A. Deptula, "A New Era for Command and Control of Aerospace Operations," *Air and Space Power Journal*, July-August 2014, 11, http://www.airpower.maxwell.af.mil/digital/pdf/articles/2014-Jul-Aug/SLP-Deptula.pdf.
[26] John J. Schaefer, III, "Responsive Close Air Support," *Joint Forces Quarterly* 67, 4th Quarter, 2012, 92.
[27] Blaker, "Arthur K. Cebrowski," 129.
[28] Cebrowski and Gartska, "Network-Centric Warfare," 9.
[29] Sean Lawson, *Nonlinear Science and Warfare: Chaos, Complexity, and the U.S. Military in the Information Age*, (New York, NY: Routledge, 2014), 121.
[30] Cebrowski and Gartska, "Network-Centric Warfare," 5-6.
[31] Ibid., 6.
[32] Erik J. Dahl, "Net-Centric Before its Time: The Jeune École and Its Lessons for Today," *Naval War College Review*, Autumn 2005, Vol 58/4, 129, https://www.usnwc.edu/getattachment/edeeb449-27f2-4eff-a18e-79be97c106de/Net-centric-before-Its-Time--The-Jeune-Ecole-and-I.aspx
[33] Micah Zenko, "Millennium Challenge: The Real Story of a Corrupted Military Exercise and its Legacy," War on the Rocks, Nov 5, 2015, http://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/.
[34] Alberts, *Network Centric Warfare*, 175.
[35] Zenko, "Millennium Challenge."
[36] J. Stiehm, *The U.S. Army War College: Military Education in a Democracy*, (Philadelphia: Temple University Press, 2002), 6.
[37] Northrop-Grumman, "X-47 UCAS Makes Aviation History...Again!" press release, http://www.northropgrumman.com/Capabilities/x47bucas/Pages/default.aspx (accessed 30 Dec 15).
[38] Lewis Hunsacker, "ARSENL Reaches Its Ultimate Goal of 50 Autonomous UAVs in Flight," US Navy, http://www.navy.mil/submit/display.asp?story_id=90863 (accessed 30 Dec 15).
[39] Robert Haddick, "Stopping Mobile Missiles: Top Picks for Offset Strategy," *Breaking Defense*, 23 Jan 2015. http://breakingdefense.com/2015/01/stopping-mobile-missiles-top-picks-for-offset-strategy/.
[40] Tyler Rogoway, "The Pentagon's Flying Decoy Super Weapon Is About To Get Much Deadlier," *Foxtrot Alpha*, Dec 11, 2014, http://foxtrotalpha.jalopnik.com/the-pentagons-flying-decoy-super-weapon-is-about-to-get-1669729445.
[41] Headquarters United States Air Force, *USAF Future Operating Concept: A View of the Air Force in 2035*, (Washington, DC: Headquarters United States Air Force, September 2015), 21.
[42] Barry Jaruzelski, Kevin Schwartz, and Volker Staack, "Innovation's New World Order," *Strategy + Business*, October 27, 2015, http://www.strategy-business.com/feature/00370?gko=e606a.
[43] Matt O'Brien, "Facebook, Google Locked in Stratosphere Race," *San Jose Mercury News*, Nov 28, 2015, http://www.mercurynews.com/business/ci_29177300/google-facebook-race-build-high-altitude-aircraft.

Bibliography

Alberts, David S. *Network Centric Warfare*. DoD C4ISR Cooperative Research Program, Feb 2000.

Aspen Strategy Group. *Balancing National Security Objectives in an Uncertain World (An Aspen Strategy Group Report)*. University Press of America, 1989.

Blaker, James. "Arthur K. Cebrowski: A Retrospective." *Naval War College Review* 59, no. 2 (Spring 2006): 129-145. https://www.usnwc.edu/getattachment/d1c5384c-f7fa-41b7-a6e6-490450835809/Arthur-K--Cebrowski--A-Retrospective---Blaker,-Jam.aspx.

Cebrowski, Arthur K. and John J. Gartska. "Network-Centric Warfare: Its Origins and Future." *Proceedings* (January 1998). http://www.kinection.com/ncoic/ncw_origin_future.pdf.

Dahl, Erik J. "Net-Centric Before its Time: The Jeune École and Its Lessons for Today." *Naval War College Review* 58 no. 4 (Autumn 2005): 109-135. https://www.usnwc.edu/getattachment/edeeb449-27f2-4eff-a18e-79be97c106de/Net-centric-before-Its-Time--The-Jeune-Ecole-and-I.aspx.

Daniel, J. Furman, III. "Through a Glass, Darkly: Strategic Perspective(s) for an Uncertain World." *Orbis* 59, no. 2 (Spring 2015): 287-294.

Dempsey, Martin E. "Transcript: Gen. Martin Dempsey at Disrupting Defense." The Atlantic Council, May 14, 2014, http://www.atlanticcouncil.org/news/transcripts/transcript-gen-martin-dempsey-at-disrupting-defense.

Deptula, David A. "A New Era for Command and Control of Aerospace Operations." *Air and Space Power Journal* (July-August 2014): 5-16. http://www.airpower.maxwell.af.mil/digital/pdf/articles/2014-Jul-Aug/SLP-Deptula.pdf.

Department of Justice. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Department of Justice, May 19, 2014. http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Dunford, Joseph F. "Center for a New American Security/Defense One National Security Forum." Comments from the Chairman of the Joint Chiefs of Staff. Center for a New American Security, Washington, DC, 14 Dec 15.

Eliot A. Cohen. *Net Assessment: An American Approach: Jaffee Center for Strategic Studies (JCSS) Memorandum No. 29*. Tel Aviv, Israel: JCSS, April 1990.

Haddick, Robert. "Stopping Mobile Missiles: Top Picks for Offset Strategy." *Breaking Defense*, 23 Jan 2015. http://breakingdefense.com/2015/01/stopping-mobile-missiles-top-picks-for-offset-strategy/.

Headquarters United States Air Force. *USAF Future Operating Concept: A View of the Air Force in 2035*. Washington, DC: Headquarters United States Air Force, September 2015.

Hunsaker, Lewis. "ARSENL Reaches Its Ultimate Goal of 50 Autonomous UAVs in Flight." US Navy, http://www.navy.mil/submit/display.asp?story_id=90863 (accessed 30 Dec 15).

Jaruzelski, Barry, Kevin Schwartz and Volker Staack. "Innovation's New World Order." *Strategy + Business*, October 27, 2015. http://www.strategy-business.com/feature/00370?gko=e606a.

The Joint Chiefs of Staff. *The National Military Strategy of the United States of America 2015: The United States Military's Contribution to National Security*. Washington DC: The Joint Chiefs of Staff, June 2015, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

Krepinevich, Andrew F. *Defense Investment Strategies in an Uncertain World*. Washington, DC: Center for Strategic and Budgetary Assessment, 2008. https://www.google.com/url?q=http://www.csbaonline.org/4Publications/PubLibrary/R.20080821.Defense_Investment/R.20080821.Defense_Investment.pdf&sa=U&ved=0ahUKEwifgMKy34PKAhUBbSYKHb7SBmsQFggFMAA&client=internal-uds-cse&usg=AFQjCNFLILxhXpNR_ey2IwUMZ2cC_ZZBYA.

Laughland, Oliver. "FBI director stands by claim that North Korea was source of Sony cyber-attack." *The Guardian*, 7 Jan 2015. http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey.

Lawson, Sean. *Nonlinear Science and Warfare: Chaos, Complexity, and the U.S. Military in the Information Age*. New York, NY: Routledge, 2014.

Manyin, Mark E. *Pivot to the Pacific? The Obama Administration's "Rebalancing" Toward Asia*. Washington, DC: Congressional Research Service report, March 28, 2012. https://www.fas.org/sgp/crs/natsec/R42448.pdf.

Mugg, James. "Jet Fighter Costs: A Complex Problem." *The Strategist*, 21 Sep 2015. http://www.aspistrategist.org.au/jet-fighter-costs-a-complex-problem/.

Northrop-Grumman. "X-47 UCAS Makes Aviation History…Again!" press release, http://www.northropgrumman.com/Capabilities/x47bucas/Pages/default.aspx (accessed 30 Dec 15).

O'Brien, Matt. "Facebook, Google Locked in Stratosphere Race." *San Jose Mercury News,* Nov 28, 2015. http://www.mercurynews.com/business/ci_29177300/google-facebook-race-build-high-altitude-aircraft.

Owens, William A. "The Emerging U.S. System-of-Systems." *Strategic Forum* 63 (February 1996). www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394313.

Rogoway, Tyler. "The Pentagon's Flying Decoy Super Weapon Is About To Get Much Deadlier." *Foxtrot Alpha*, Dec 11, 2014. http://foxtrotalpha.jalopnik.com/the-pentagons-flying-decoy-super-weapon-is-about-to-get-1669729445.

Sanger, David and Rick Gladstone. "Piling Sand in a Disputed Sea, China Literally Gains Ground." *New York Times*, 8 Apr 2015. http://www.nytimes.com/2015/04/09/world/asia/new-images-show-china-literally-gaining-ground-in-south-china-sea.html.

Schaefer, John J. III. "Responsive Close Air Support." *Joint Forces Quarterly* 67 (4th Quarter, 2012): 91-96.

Stiehm, J. *The U.S. Army War College: Military Education in a Democracy*. Philadelphia: Temple University Press, 2002.

Stockholm International Peace Research Institute. "SIPRI Military Expenditure Database." Stockholm International Peace Research Institute. http://www.sipri.org/research/armaments/milex/milex_database/milex_database (accessed 15 Mar 15).

Sweetman, Bill. "New Radars, IRST Strengthen Self-Detection Claims." *Aviation Week and Space Technology*, Mar 16, 2015. http://aviationweek.com/technology/new-radars-irst-strengthen-stealth-detection-claims.

US Census Bureau. "US Trade in Goods and Services – Balance of Payments (BOP) Basis." US Census Bureau, Economic Indicator Division, Feb 5, 2016. http://www.census.gov/foreign-trade/statistics/historical/gands.pdf.

US Department of Defense Press Operations. "Department of Defense Selected Acquisition Reports (SARs) (As of December 31, 2014)." News release no. NR-090-15, March 19, 2015. http://www.defense.gov/News/News-Releases/News-Release-View/Article/605423/department-of-defense-selected-acquisition-reports-sars-as-of-december-31-2014.

The World Bank. "GDP at Market Prices (current US$)." The World Bank, http://data.worldbank.org/indicator/NY.GDP.MKTP.CD (accessed 30 Dec 15).

The World Bank. "Military expenditure (% of GDP)." The World Bank, http://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS (accessed 30 Dec 15).

Zenko, Micah. "Millennium Challenge: The Real Story of a Corrupted Military Exercise and its Legacy." War on the Rocks, Nov 5, 2015. http://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/