The Future of Warfare

Mr. Frank Kendall

November 11, 2024

Contents

Dedication

To the brilliant men and women at DARPA with thanks for all the great work they do every day to create technology that contributes to our security, and to all American service members for their willingness to risk and even sacrifice their lives in defense of our country and the values for which it stands.

Acknowledgements

With special thanks to Steve Walker and Peter Highnam of DARPA for giving me the opportunity to put down these thoughts in a classified setting at DARPA and to all the many people whose wisdom, knowledge and experience contributed over the past half century to the ideas expressed herein.

Preface

This work is a culmination of several decades of studying, working on, and thinking about the intersection of technology and organized violent human conflict. We are living in an age of exponential technology development that is certain to have a profound effect on how any future conflicts will be fought. We are also living in an age in which a brief period of American dominance in conventional warfare may be coming to an end. I do not believe that the implications of those emerging technologies or how they will impact American military power have been adequately explored or defined. This paper will certainly not be the final answer to the question of how future wars, especially wars between great powers, will be fought and won, but my hope is that it will stimulate additional analysis (especially quantitative analysis), technology maturation, and experimentation that will point the way forward more clearly. I have confined this paper to the subject of conventional warfare between major economic powers, leaving strategic nuclear conflict, weapons of mass destruction in general, counterinsurgency, and counterterrorism largely to others or another time, although I do address these topics briefly. Initially my intent was to write a somewhat abstract and generic paper, but as the work progressed it became increasingly difficult to avoid taking a US-centric perspective. I finally concluded that the best course was to accept that the problem I was really most interested in was the erosion of US conventional military superiority, something I've been sounding the alarm about for over a decade. Much of what I discuss is generic and could apply to any nation's conventional military, but I have also felt compelled to address the unique situation faced by the US as a great power with major military alliance commitments oceans and continents away. The US has global interests to protect and potential adversaries who have been actively working to acquire the means to defeat our ability to project conventional military power far from our shores. During the early decades of my career, the United States faced one such problem, the Soviet Union, and one likely theater of war, Europe. Today we face two major threats, China and Russia, and two vastly different theaters, the Western Pacific and Europe. There is arguably an analogy between today and the WWII era when we faced Germany in Europe and Japan in the Pacific, but technology has dramatically changed the implications of time and distance and the environment in which we confront the strategic threats of this century.

In the US, DARPA has led that technological charge, with some more tentative advances taking place in the military services as well. Internationally, the development of and the operational movement toward manufacturing and employment of lethal autonomous systems, and their effectiveness against legacy concepts has been even more aggressive. The recent conflict in Armenia has provided an operational demonstration of some of the relevant technologies.

As I completed this work, I was left with two important impressions that I would like to mention here. Both are indicative of critical needs in the human side of the future of warfare. While I have emphasized autonomy, in particular lethal autonomy, in this paper, I have always left an important controlling role for humans. This role manifests itself at an echelon or two above that where individual engagements occur. Humans may not do the actual fighting in the future operational concepts that I imagine, but they will be critical to successful outcomes, making their judgment, skills, and preparation a paramount concern. Second, I envision future conventional conflict to be violent at scale and to involve the full range of adversaries' power in an attempt to achieve prompt and decisive victory. Our peer or near peer future adversaries will not come at us with measured and tentative commitments, but with all that they have. I believe that our ability to deter or defeat aggression will depend on our ability to field forces significantly more operationally effective than our enemy's, and on our skill in employing them at scale in a violent full spectrum environment. What follows are my thoughts on what that might look like. It is not just a technical

and operational story; I couldn't resist weaving in some of my own experiences over the years where I thought they were relevant. I hope readers will not find these digressions too distracting.

Update

A word on the timeline of this paper. This is a work that I began mentally composing when I left government service in early 2017 and largely completed before taking office as Secretary of the Air Force in the summer of 2020. The views within are thus my own and do not represent the official position of the Department of the Air Force or the Department of Defense. However, I would offer two observations on the continued relevance of this line of thinking. First, it has been interesting to observe the progress of technology, experimentation, and innovative thinking by others all moving rapidly down the general path I will describe here. While I continue to believe that we are "out of time" to implement the concepts herein from a technological, organizational, and doctrinal perspective, I am heartened by the significant movement already underway. Second, the experiences of the last four years have served to reinforce my belief that these concepts are directionally correct. For example, technologies that were demonstrated in Armenia have been further developed by innovative Ukrainians and proven at scale in the conflict with Russia; UAVs employed by ISIS as asymmetric threats to US forces in Syria have evolved into one-way attack vehicles threatening shipping in the Red Sea. The cycle of innovation and response only accelerates, and I continue to believe that the appropriate response is to master technological change rather than resisting it.

Introduction

Some History, Personal and Otherwise

I hate war. It is the most wasteful and cruel of human endeavors. And yet I have chosen to spend most of my life either in uniform or working on weapons system development programs as a civilian. I made this choice because I felt that the United States was a leader in the world for things worth fighting for, not just America's narrow interests, but also ideas, values, and principles that were worth defending in their own right. I still feel that way. I started adult life as a cadet at West Point during the Viet Nam War. I grew up on the shadow of WW II and the Korean War. The first twenty years of my career were dedicated to the cause of winning the Cold War against Soviet style authoritarianism. The last ten years were dedicated to the cause of responding to the threat to human freedom posed by new authoritarians in China, to a lesser extent Russia, and by religious zealot's intent on imposing their beliefs on others by force. I am hopeful, but not optimistic, that we humans will find another way to resolve disputes between nations than violent confrontation. Until that happens, those of us who live in freedom need to be prepared to defend that freedom.

This paper will be about the intersection of technology and military operational concepts. This intersection has been the focal point of most of my career. Technology moves forward at the pace of human discovery and invention. It can be stimulated by the desires and vision of military operators and others, but generally technology emerges from the endless human search for knowledge which has its own momentum, driven by an array of motivations. Once discovered or created, technology serves as an enabler that drives changes in warfare. It affects the types of force structures that will be acquired, the equipment those forces will use, and how those forces will fight. The history of warfare (how militaries are organized, equipped, and fight—not the history of battles) is the history of the pursuit of operational advantage, something that changes constantly, and sometimes dramatically, with the emergence and application of new technology. Transformative technologies can render whole classes of equipment and the forces that use them obsolete almost overnight. Ironclads signaled the end of the wooden ship navies of the world. The longbow, crossbow and musket signaled the end of mounted armored knights. Airplanes signaled the end of the battleship. Precision munitions (missiles predominantly) are currently having an uncertain and still incomplete impact on weapon systems and operational concepts. Looming directly in front of us are the implications of lethal autonomy and artificial intelligence.

My government service spanned a lot of history, particularly two periods of roughly 8 years apiece in the acquisition and technology organization of the Office of the Secretary of Defense, separated by fifteen years in defense industry. The first stint spanned 1986 to 1994—including the last few years of the Cold War and the First Gulf War. The second period spanned 2010 to 2017—a period taken up by conflicts in the Middle East and Afghanistan, but also by increasing awareness of the threat posed by a rising China and a revanchist Russia. I worked hard during this later period to raise the alarm about the military modernization programs being pursued by China, and to a lesser extent by Russia. Because of its resources, regional and global ambitions, and authoritarian system of government, China is the greatest strategic threat to the United States and to the liberal

democratic order established by the United States after WW II. My experiences have given me the opportunity to participate in endless analysis, discussion, and debate about the best technology investments and the best operational concepts for the United States to adopt, in all domains of warfare. It is this combination—technology and operational concepts (applied with thorough preparation and professional execution)—that determines success in warfare and defines the evolution of warfare from one era to the next. At this time there is a growing awareness of the technologies that will profoundly change warfare in the next decade or two, particularly autonomy and some forms of so-called artificial intelligence, but very little understanding of how those technologies will be operationalized, and no commitment to taking the steps needed to achieve that goal at scale.

Our great victory in the Cold War came about peacefully as a result of a superior economic system that enabled, among other things, numerous advances in the application of technology to warfare. Some would credit the Reagan-era Strategic Defense Initiative (SDI) for breaking the back of the Soviet economic system. I worked extensively on the SDI program for several years. It was always ambitious to the point of irrationality. More pragmatic, and more demonstrably successful was the Follow-on-Forces Attack (FOFA) program which grew out of a DARPA concept demonstration set of experiments called Assault Breaker. FOFA was a direct challenge to the Soviet echeloned mechanized forces operational concept. The FOFA suite of wide area surveillance systems (especially JSTARS) combined with precision munitions, and connected in a supporting data network, plus the introduction of stealth technology, proved in the First Gulf War to be truly revolutionary. Whatever the motivator or impetus to the Soviet collapse, there was no doubt after 1991 that the US had revolutionized conventional warfare. Unfortunately, and for several reasons, we cannot count on our Cold War history to repeat itself against our new competitor, China, and to a lesser extent against Russia.

The quest for military advantage based on the application of technology is a constant in the history of warfare. What makes the last century and the current one unique relative to earlier eras is the pace of technological change in general, military and civilian. What makes our current time unique is the transformational effect that specific new commercially-based (as opposed to military unique) technologies will have on warfare. I believe the changes we will see as a result of the emergence of these commercial technologies are much more fundamental than generally perceived.

One can think of the last century of change in conventional warfare as having come about through the three waves of modernization. The first wave included the industrialization of warfare, quantum improvements in lethality, and the mechanization of warfare. WW I introduced early versions of new technologies—machine guns, long-range artillery, and barbed wire—that collectively dramatically increased lethality against advancing infantry. The participants in this conflict were roughly evenly matched in capacity to generate forces and the advantage of defensive firepower over maneuver led to stalemate and a war of attrition—carried out at industrial scale. As the war progressed the widespread use of tanks, trucks and tactical aircraft set the stage for the culmination of this first wave of modernization that was represented by WW II when those systems restored maneuver to the battlefield. At sea, long-range naval gunfire and heavy armor dominated the conflict originally, but the submarine and the aircraft carrier were introduced and became the

platforms that would be dominant in WW II. The introduction of radio communications in WW I and both Radar and Electronic Warfare (EW) were also important elements of this wave of modernization. The operational concept embodied in the "Blitzkrieg" concept became the accepted norm during WW II. It was sharpened and reached its culmination in the United States' "Air-Land Battle" doctrine of the 1980s. I had the privilege as a junior officer to serve under and later to work closely with the principal architect of Air-Land Battle, US Army General Donn Starry.

The next wave of modernization is the one the United States introduced in Iraq and Kuwait in 1991 and has used repeatedly since. It remains the underpinning set of capabilities the United States still employs. This suite of capabilities, which originated in a DARPA demonstration program, appliques wide area surveillance, precision munitions—especially stand-off missiles, and networked digitized command and control onto the WW II era mobile mechanized warfare construct. More accurately it integrates those technologies onto the "Air-Land Battle" construct of the Cold War. From 1989 to 1994, I was the Deputy Director of Defense Research and Engineering for Tactical Warfare Programs in the Office of the Secretary of Defense. One of several organizations that reported to me was an office dedicated to "Follow-On Forces Attack" or FOFA programs that included the main building blocks of this wave of modernization. Included were the JSTARS wide area ground surveillance sensor and several air and artillery delivered precision munitions. With strong advocacy from the Defense Science Board (particularly Gene Fubini and Joe Braddock) these programs were managed as a separate portfolio because of their revolutionary and interdependent importance, originally to defeating multiple echelons of Soviet armor.

In the 35 years between WW II and the First Gulf War a number of other innovations were embraced, but without as fundamental an impact. Aircraft made the transition from propeller to jet propulsion. Satellite systems came into existence and provided intelligence and communications support. Helicopters came into wide-spread use, for attack, reconnaissance and maneuver or transport applications. Integrated virtual and live training systems for large ground formations and many-on- many aerial engagements also improved dramatically. Stealthy aircraft were introduced by the United States in the First Gulf War, a significant advance, but not one with fundamental operational concept implications. At sea, the dominance of the aircraft carrier and the submarine appear to have continued, but with significant evolutionary upgrades. None of these innovations changed the fundamental nature of conventional warfare, however.

It can reasonably be said that Dwight Eisenhower, Douglas McArthur, Chester Nimitz, Hap Arnold or Alexander Vandegrift would have no trouble understanding the composition of today's American military and how it conducts large scale conventional operations. That's an oversimplification, but there is a significant element of truth in it. The basic building blocks are highly similar, and where technology has enabled changes, those changes could be understood in operational contexts familiar to the ones employed by these leaders from 75 years ago. What would most surprise all of those leaders, is the relatively low loss rates in combat to which the United States has become accustomed. In the First Gulf War we expected thousands and even tens of thousands of casualties. Both there, and in other significant operations since, such as the second assault on Iraq in 2003 and the air campaign in Serbia in 1999, losses of both machines and people

for the United States and its partners have been extremely low.[1] That era, unfortunately, is coming to an end.

After the United States demonstrated the revolutionary efficiency and effectiveness of its conventional forces in Iraq in 1991, all our potential adversaries took notice, but none more so than China. While the United States was entering a period of both recognized military dominance and complacency about the degree to which that dominance would endure, China began to study how it should best respond to the American advances. Coincidentally China was also starting to become rich and would have both the resources and insight needed to challenge the United States' ability to project power. China has now reached something close to parity with America in Gross Domestic Product and will soon exceed the United States by that measure. When I briefed then National Security Advisor Susan Rice on Chinese military modernization in 2015, she seemed surprised when I told her I was far more worried about China than Russia. Military power flows from economic power, as do strategic ambitions, and China is vastly more economically powerful than Russia.

For the most part, China has emulated the United States as it has worked to modernize its forces. The Chinese have developed and fielded precision munitions, wide area surveillance systems, and networking. China has lagged behind the United States to some degree, but through a combination of theft and intelligent strategic resource application it has significantly closed the gap in the quality of its fielded capability. Also, China has already developed, or is in the process of developing, a range of capabilities that are well chosen to reduce or eliminate US advantages. These include a suite of more capable air-to-air missiles, electronic warfare systems, and anti-satellite systems. What has most distinguished China's modernization program, and focused my attention, is the degree to which China has strategically targeted America's ability to project conventional military power close to China.

Unconstrained by the Intermediate Nuclear Forces Treaty, which banned ground launched conventional as well as nuclear weapons between 500 and 5,500 kilometers in range for the U.S. and Russia until the US withdrew in 2019, China has emphasized long-range precision conventional missiles, both ballistic and cruise. The reason for this Chinese emphasis is America's dependency on a small number of high value assets to conduct power projection. Those assets include aircraft carriers, regional fixed air bases, military satellites, and a few logistics and C2 nodes. China complements its large inventory of ground-based missiles with air and ship-based systems as well. The short version of the current situation is that the United States is the dominant military power until within about 1,000 miles of China, and then things begin to change.[2] That number is growing over time as China fields more capability, but it is already large enough to make it problematic for the United States to meet its security commitment to regional allies. China, however, is not pursuing a new wave of modernization per se; they are investing in the same

[1] Counterinsurgency campaigns have continued to extract high numbers of casualties. By their nature they are wars of attrition and put defenders at risk as they are forced to move among the population while trying to suppress insurgent groups and provide security to civilian society.

[2] This was how I described the situation to then National Security Advisor Susan Rice in 2015.

technologies and concepts the United States introduced, just in a way that is tailored to their most important operational military problem—keeping the United States out of their part of the globe.

The recognition of this problem, which is well beyond "emerging" at this point, led to a number of initiatives over several administrations. Almost immediately after I returned to the Pentagon in March of 2010 it became clear to me that we had a big problem. As I reviewed daily intelligence summaries on China's military modernization programs their strategy became obvious to me. I started to raise the alarm, but I confronted two problems in getting the Department's attention. The first was that we were still heavily engaged in Afghanistan and Iraq. The second was that the idea that the conventional forces of the United States could be challenged, let alone challenged successfully, was an alien and almost unacceptable concept to even articulate. The antibodies were strong, even when confronted with direct evidence. I continued to beat the drum, internally and externally in speeches, in testimony (both classified and unclassified) and in internal budget deliberations. On more than one occasion very senior people asked (directed) me to reduce the volume of the alarms I was sounding. By then I was so on the record publicly, including in Congressional testimony, that I could not do so, even if I had wanted to.

There were some efforts in the Defense Department to address the problem of China's modernization program and the rising strategic threat China was becoming. When I returned to the Pentagon in 2010 there was already a group called the "Long Term Competitive Strategies Group" working on the China problem. It was led by Michelle Flournoy, USD for Policy, and General "Hoss" Cartwright, VCJCS. I quickly joined this group and formed a "Research, Development and Acquisition Task Force" led by Al Shaffer, PDASD for Research and Engineering, to support the effort. Later, when we developed a new National Defense Strategy under Secretary of Defense Panetta, it reflected a shift to emphasize the Asia Pacific region. The Obama Administration asserted that this shift was not about China, but of course it obviously was. Secretary Ash Carter later made great power competition one of the themes of the 2017 defense budget the Obama Administration submitted. He emphasized five threats; in order they were China, Russia, North Korea, Iran, and extremist groups, The Trump administration, in its National Security Strategy and National Defense Strategy, echoed this shift and increased the emphasis on great power competition.

The primary way the focus on great power competition manifested itself in the Trump administration was an obsession with speed in acquisition programs. I believe this was a serious mistake for two fundamental reasons. The first is that "haste makes waste." Trying to do an acquisition program faster than it can reasonably be completed has historically led to failure in the form of large schedule and cost overruns and nothing entering the inventory. History is full of examples (FCS, A-12, FIA, SIAP) that prove this point, but facts and data never seem to overcome the unfounded optimism of amateurs with what they think is a new idea for how to acquire weapon systems. The second is that going in the wrong direction fast doesn't actually get you closer to your goal. We are in a strategic long-term competition with China and arguably with Russia. We normally keep the weapons and other military systems we buy in our inventory for decades. If we expect to continue to do that, then it's important that they be cost effective and designed for the

needed service life. The rush to field existing technology in immature designs is inconsistent with both of these objectives.

Perhaps the most visible attempt to counter China's modernization program was the so-called "Third Offset Strategy." This initiative was created by Deputy Secretary of Defense Bob Work during the final years of the Obama Administration. It was based on the idea that the US had successfully implemented two earlier offset strategies and needed a new one. The first of these was the fielding of thousands of low yield tactical nuclear weapons in Europe to counter the threat of overwhelming formations of massed Soviet armor. After WW II the US and its allies had largely demobilized, and did not have conventional forces large enough to compete with those of the Soviet Union. What the US did have was a short-lived monopoly on nuclear weapons. This "first offset strategy" was considered successful, until the Soviets started fielding their own nuclear weapons. The "second offset strategy" was the second round of conventional warfare modernization commented on earlier. In this offset strategy the combination of precision weapons and battlefield awareness was intended to defeat the same massed Soviet armor. The problem Bob Work correctly perceived was that with the proliferation of precision munitions the second offset strategy would lose its comparative advantage. He was basically right about this; the US is more vulnerable to long-range precision munitions than our adversaries because we project power far from our shores utilizing forces that depend on small numbers of very capable but expensive and targetable assets.

In the summer of 2015 several of us worked with Bob Work to try to define the content of a third offset strategy. That group included Bob Work, VCJCS Admiral Sandy Winnefield (later General Paul Selva), Defense Science Board Chair Craig Fields, DARPA Director Arati Prabhakar, Assistant Secretary of Defense (ASD) for Research and Engineering Steve Welby, Acting ASD for Acquisition Jimmy MacStravic, and myself. We met for three or four hours on several occasions to consider options and review information from various sources. During this period, I also initiated a "Long-range Research and Development Program Planning Study" led by Steve Welby. At the end of all this work we had come up with three features we thought would be central to a third offset strategy: range, autonomy, and quantity at cost. I still think this is the right formulation, and that it can apply in multiple domains. Our work was incomplete however, in that we never defined how these principles would be operationalized. What would we actually build and how would those components interact in an operational concept? Without answers to those questions, we were left with the idea of a third offset strategy, but no clear definition of what it was and no actionable plan to implement it. This paper is an attempt to move that work forward and to present some more specific ideas about what the next, pick your phrase, Military Technological Revolution, Revolution in Military Affairs, or Offset Strategy, will actually consist of in meaningful operational and technical terms.[3]

[3] As an aside, at the conclusion of our efforts, Bob Work built a briefing around autonomy alone and started to present it as the result of the third offset effort. Bob's product provided a general description of how autonomy and artificial intelligence of various types would transform warfare, but it was abstract and very generic. There was still no clear description of what would actually be built or how the components would work together in an

Fundamentals

Let's ignore the notions of offset strategies or revolutions in military affairs for now and focus more directly on military fundamental attributes and the dominant variables in conventional warfare. I don't want to get bogged down in semantics or taxonomy here, but it's useful to start with a logical framework so that a reader will understand the origins of some of my thinking once I get into specifics.

All attempts to achieve technology based military advantage are rooted in some combination of fundamental attributes and variables that affect military success. All major improvements in military performance are also ultimately about some form of greater operational efficiency that has its origins in advantages in superior attributes or relative control over dominant variables. In operations research terminology this all manifests itself in exchange ratios; kill ratios and cost exchange ratios. If one side can find a way to better destroy the other side's assets while losing less of its own, in both quantity and cost metrics, than that side has an advantage. If this gap is wide and difficult to overcome, the advantage is almost certainly decisive. A very recent example of achieving high-cost exchange ratio efficiency may have been the successful use of inexpensive drones to attack Armenian armor in the conflict between Armenia and Azerbaijan in the summer of 2020. Historically, and for the US, the first two so-called offset strategies provide good examples, but with very different approaches to achieving operational efficiency. The first offset strategy increased operational efficiency through the ability of a single expensive weapon, a nuclear weapon, to kill a lot of enemy platforms and people. The second offset strategy increased efficiency by using a lot of relatively inexpensive, but very accurate, individual weapons to kill a single platform—one shot, one kill. Both modern offset strategies were about achieving cost effective lethality, but by using the opposite approaches.

Overall, what attributes and variables drive operational efficiency metrics? The attributes of most direct significance are cost, lethality, and survivability. These in turn are all coupled to advantages in range and speed, and in detection and concealment. Every one of these variables or attributes is connected and dynamic, but let's consider each briefly, and consider the US' current posture with regard to these parameters. All these variables, and many others, must be traded-off with each other in design studies and analysis. My trade-offs in this paper will unfortunately be intuitive based on my decades of experience doing and studying operational analysis. If time permits and DARPA is willing, my hope is that this paper will lead to deeper, more analytical trade studies. The Department of Defense desperately needs to increase its capacity to conduct operational analysis and hopefully this effort will stimulate more of that work.

Let's start with cost. Cost is usually measured in absolute terms (dollars), but in practice relative cost is what matters. A good example is using a $100,000 air-to-air missile to shot down a $1,000 drone as opposed to using the same missile to shoot down a $50 million tactical aircraft. There are some other complicating factors when one analyzes cost, however.

---

operational concept. Importantly, Bob declined to include range and quantity at cost as equally important parameters with autonomy and artificial intelligence. I believe these were important omissions.

One of those factors is that cost isn't a perfect measure of value. Value assessments have a non-linear quality. Think of it this way—the first and last aircraft carrier in the inventory may have similar costs, but as carriers are lost in combat and can't be replaced the operational value of the remaining assets increases substantially. The "cost" in operational terms of an incremental loss increases disproportionately and nonlinearly as the asset pool shrinks. Also, if we only have one of something and we lose it, the cost of that loss is 100% of that capability. If we can't replace that system for a matter of years, the operational cost of that loss could be very high because of the overall impact it would have. I believe the U.S. has this problem in spades today because we are very dependent on a small number of assets for critical functions. Independent of their dollar cost or even their cost exchange ratio, these assets have enormously high value in our operational plans and concepts of operation. Loss of these assets, or a high fraction of them, could lead to operational or even strategic failure very quickly.[4]

In addition to cost in dollars, there is also cost in human lives. The US may have a significant and enduring disadvantage when it comes to our asymmetric valuation of human life compared to opponents. To our credit, we are reluctant to expend large numbers of American lives. Our experience for the last few decades has been with operations that have involved comparatively low numbers of casualties. This is a relatively recent development. We had over 50,000 causalities in Viet Nam. We expected over 10,000 casualties in the First Gulf War. We shocked ourselves, in a good way, with the efficiency improvements we had built into our Joint Task Force in Kuwait and Iraq in 1991. We did experience significant losses in Iraq and Afghanistan counter-insurgency campaigns, but not on the scale of previous major conflicts. We bore those losses, but we also took extraordinary measures to reduce them. My guess is that if the motivation for the conflict was strong enough, the US could still accept high losses to achieve a vital national military objective, but this proposition hasn't been fully tested for the current generation or for an all-volunteer force.

We also have a cost problem of a related but slightly different nature for another reason within the systems that we have in higher quantities, such as aircraft and surface ships. It may be unlikely that we would lose a high fraction of these higher quantity assets in the opening hours or days of a conflict. However, at reasonably foreseeable exchange ratios against a peer competitor, these forces would be fairly quickly exhausted. Even modest attrition rates become unacceptable very quickly when measured in the fraction of our capacity that would be consumed in continuous operations over just a few weeks. A good example is the acceptable loss rate for continuous air operations, such as those waged over Germany in WW II or North Vietnam during that conflict. The problem is compound interest in reverse. A loss rate of 1-2% a day in continuous operations may be acceptable on a given day, but over consecutive days it consumes a force very quickly.

In a study I participated in at CSIS led by Kathleen Hicks (then at CSIS), we reviewed some alternative future force structures that had been hypothesized under different defense budget assumptions. The minor epiphany struck me that even the largest of the forces being considered could not sustain anything near historic loss rates in a protracted conflict, either episodically or

[4] My suspicion is that this situation exists today and already limits our practical operational options in some real-life scenarios, and therefore weakens our conventional deterrent substantially.

through continuous attrition. As with the high value, small quantity assets discussed above, the replacement time for the systems in our inventories is measured in years. The implications of this situation are strategically significant. We cannot solve this problem with the resources we have if we continue to buy the types of tactical systems we've been buying for decades. It's worth thinking about our solution to this same problem during the Cold War when we were trying to stop a Soviet Invasion of West Germany. Even though we had significantly higher fielded inventory and much more force structure than today, we still assumed we would fall back on tactical nuclear weapons when the conventional force was about to be overwhelmed. Today we don't even have that disturbing option.[5]

Let's move on to lethality and survivability. These variables are inherently relative and measured in relation to specific threat capabilities. They tend to be thought of on a weapon and platform basis respectively, and that's a good place to start, but force lethality and survivability are also important and bring in added complexity. The armor protection versus anti-armor munitions contest of the Cold War is a good example of the platform versus weapon perspective. This contest was an exercise in continuous incremental competitive improvements in lethality and survivability on both sides. But these attributes can be measured on a system-by-system basis or for forces consisting of combined systems. For example, just the addition of JSTARS to the First Gulf War battlefield dramatically improved the lethality of the US led coalition force.[6] Lethality and survivability metrics are quantifiable at both levels and lend themselves well to comparative analysis and trade-offs. Former Secretary of Defense Jim Mattis strongly emphasized improving lethality of US forces during his tenure as Secretary. I'm a huge admirer of Jim Mattis, but I think he got this wrong; US forces have a much bigger problem with survivability than with lethality. I also think there is a strong cultural bias in any military, US or otherwise, currently and historically, to discount vulnerabilities that implicate a military organization's sense of identity. It often takes a shocking operational event to force this recognition, and sometimes even that doesn't do the trick—examples are legion.[7]

There are other variables to consider. Range, or the ability to act from longer range then the enemy—to both see and kill from farther away has been at the heart of many if not most major advances in warfare over all of human history. Range can confer survivability, but it is only of value in improving operational efficiency if adequate lethality and acceptable survivability and cost are also available with the increased range. Speed, and here I'm referring to speed of movement or speed to deliver effects that derives from certain physical features originating at the

[5] I'm not recommending that we rebuild the tactical nuclear forces of the '70s and '80s, but we should think carefully about the implications of this situation. I'll leave that problem for another paper, but my preliminary thought is that we should aim for a conventional deterrent with the ability to defeat any likely adversary act of military aggression operationally. This is as opposed to keeping a force in being with the ability to win a protracted conventional conflict.

[6] I was part of a group that fought successfully to get the two JSTARS developmental prototypes sent to the Gulf, over the objection of the Air Force, which didn't want to disrupt the test program. My favorite quote from that era was the CSAF after the war who said, "We will never go to war without JSTARS again."

[7] At the outset of WW II the commander of US Army cavalry is reported to have written CSA George Marshall to argue that increasing the size of the cavalry branch was the key to winning WW II.

platform or weapon system level (such as super-cruise as in the F-22 or most recently hypersonic propulsion) has value. It confers the superior ability to create or shorten range and in the aggregate the ability to maneuver forces more rapidly, implying the ability to, in the much-overused phrase, "move to a position of advantage." An ageless adage for fighter pilots is "speed is life" referring to the value of the superior ability to separate from or close with an adversary in aerial combat. Superior speed of movement has military value, but it is very context dependent and usually does not provide an enduring advantage because adversaries can emulate major advances in this area relatively quickly.

Another, and neglected fundamental is sustainability, which I define broadly to encompass everything necessary to bring a force into battle and keep it effective throughout its employment. Professionals do worry about logistics, and any discussion of the future of warfare must take this into account. It's great fun to think about new operational concepts and new platforms, weapons and force structures, but that's only half the problem of conducting military operations. Forces have to be ready when needed and they have to both get to the battlefield and be supported efficiently and fully once they arrive.

Sustainment considerations are also critical to total life cycle cost. Cost considerations have to take the total cost of operating systems into account when exchange ratios and value comparisons are made. For a given weapon system, sustainment costs are generally much higher than the costs of development and comparable to or greater than the costs of production. Sustainment is the major contributor to the cost of ownership. An enormous part of the cost of our current human operator-centric military enterprise is the cost to operate and maintain the equipment and train the people associated with the equipment.[8] The current US paradigm for many systems, and the nature of modern warfare, leads to complex systems that require the almost continuous training of human crews on their own organization's equipment to maintain proficiency in very perishable human skills.

For the U.S. in particular, sustainment is part of a vicious cycle. Complex and expensive human operated systems can only be afforded in small numbers. Because they can only be afforded in small numbers and because they take a long time (years) to manufacture, they also have to be highly survivable, reliable, and field supportable so they can be kept on the battlefield throughout a conflict. All of this drives support cost up. In the US model, our platforms are also used frequently, if not continually, for training purposes, which in turn leads to continuous maintenance at the operational level punctuated by higher level depot or equivalent maintenance. Any significant upgrades have to be scheduled around the human operator peacetime operational deployment and training tempos. In wartime use, our complex manned systems must be maintained at or as close to the operational echelon as possible so that they can stay in the fight. A great deal of the current U.S. force structure, at all echelons, is necessary today to maintain relatively small numbers of actual fighting platforms, and to provide the trained and deployable people to operate them.

[8] There are several times as many people in uniform doing support work as there are actual fighters. The Army, for example is about 25% combat forces and 75% support (logistics, life support, and headquarters).

For contrast, it's interesting to compare the US and the Soviet sustainment models. The Soviets designed their systems for their expected battlefield life, not for decades of use in training. The Russian WW II experience was a very high attrition rate over a protracted period. They accepted that high losses in people and equipment would occur. It their WW II experience-based models of combat attrition indicated that a main battle tank would have a 3-day life in combat, why design it to be reliable for more than a few days? It would be destroyed by then anyway. In peacetime, the Soviets also only used a small fraction of their equipment in training, and they used the same equipment repeatedly. The balance was parked and only checked occasionally for readiness. As we think about future forces and operational concepts, we should both treat sustainment as a critical parameter and cost factor, and we should be open to new sustainment paradigms that technology might enable.

By now some readers are apoplectic that I haven't talked about decision speed and quality. The US has long emphasized decision-making superiority and the ability to conduct coordinated action more effectively than an opponent. This attribute of Command, Control, and Communications Battle Management (C3BM) is a significant contributor to relative efficiency and advantageous exchange ratios.[9] In the United States, this emphasis also dates back to the "Air-Land Battle" doctrine. It was integral to FOFA and provided the focus of both "digitization" and "network centric warfare" in the early 90s. Most recently the quest for decision speed and quality takes the form of Combined Joint All Domain Command and Control (C-JADC2) and in each of the Military Services' versions of that concept, none of which seem to me to be very well defined at this point. Decision speed and quality do matter, and they are driven by the timely availability of relevant information where it can be used and the process to turn that information into sound decisions faster than an adversary can respond. This paper will not, however, be fundamentally about the information "revolution" as I will explain below. I won't ignore C3BM, but I view that function as supporting of an operational concept, not the other way around. My view is that, with effort and attention, we can build the C3BM networks we would need to support the operational concepts I will define. C3BM and automated functionality within the networks are important design considerations and enablers, as well as potential vulnerabilities, but they won't be the central focus of this paper.

The Soviets were a little obsessed with quantified theoretical measurements of relative combat power, what they called "correlation of forces," but they also firmly believed that time was the most important variable on the battlefield. They had a point. Today's advocates of unlimited connectivity and infinite bandwidth coupled with massive computational power and artificial intelligence based human decision support want to take that point to an extreme level. I believe this visionary concept has some merit, but in addition to not being very well defined or as far as I can tell adequately supported by analysis, current concepts have at least two flaws; they don't adequately consider the degree to which the enemy has a vote and they overly value centralized human decision making.

[9] The acronym has grown over time to BMC4 (adding Computers) and C4ISR or BMC4ISR or C5ISR (adding Cyber). I'll distinguish the sensor or ISR suite from the BMC3 network that connects elements of an operational concept and supports decisions.

American's generally talk about operational decision time in terms of the Observe, Orient, Decide, and Act or the "OODA loop." The ability to control time, to move and/or take effective action faster than the opponent, is derived from the collection of capabilities that affect decision speed and quality, which is a feature of C3BM systems' performance and the Intelligence, Surveillance, and Reconnaissance (ISR) systems that feed information into those networks. In recent years American military leaders have spoken ad nauseam about the need to "engage the enemy from a position of advantage at a time and place of our own choosing." Faster and better decision making, in other words superior ISR and C3BM, provides opportunities to achieve positional advantage and enables coordinated action—all in order to provide better relative operational efficiency. In other words, the point of superior C3BM and ISR is to enable greater lethality and survivability.

This is all fine, but my view is that in the US, our rhetoric on this has been a little over the top—going all the way back to "digitization" and "network centric warfare" in the 90s, and now to "multi-domain warfare." I agree that there is improved efficiency to be obtained by aggregating and analyzing information efficiently and providing better automated command and control tools, but the enemy has a vote, and the resiliency of this approach as well as the limited potential efficiency improvements even theoretically possible lead me to believe the US may be over-relying on the concept of a military AI driven internet of things (IOT) concept for future battlefield superiority.

I have on occasion asked questions about the degree to which realistic or even ideal integrated C3BM can improve operational results. I know there are improvements to be had, but I'm concerned the almost religious faith in this concept as a panacea is misplaced. How much more survivable will JADC2 make our aircraft carriers, forward air bases and satellites? We need to quantify the operational impacts of JADC2 and more fully investigate the risks associated with responsive threats—especially kinetic threats to key nodes as well as both cyber and electronic warfare threats. It's a sure bet that our adversaries are working on all of these problems. At this point, my greatest concern in this area is assuring survivable and effective ISR systems that can find and identify targets of interest with high probability of detection and low false alarm rates–in all domains of warfare. Fusing sensor data can be very helpful at improving aggregate results, but doing so is technically challenging, requires secure high data rate communications, and high-resolution sensors with reasonably good target detection and identification performance individually.[10]

The other technology driven area in which I think our rhetoric has been over the top, but less so, is Artificial Intelligence (AI). The basket of technologies we call AI is truly transformative, and this transformation is happening quickly. I'm definitely not talking about true human-like artificial intelligence, what we think of as consciousness, which is still a long way off. I am talking about the forms of AI known as pattern recognition, machine learning, data analytics, autonomy, and executive decision making or support. All these areas have been in development for decades, but the recent and continuing pace of advance in these areas is what will make the concepts I will

[10] One notable shortfall historically is the ability to find objects the enemy doesn't want found, especially stationary objects that can be disguised and for which cheap decoys can be fielded.

describe realistic and not science fiction. I believe many of them are possible in the relatively near term—one to two decades. As we field self-driving cars and trucks, deliver packages by UAV, and start to see fully automated (if not unmanned) commercial shipping, as we see facial recognition at scale implemented on our laptops and through surveillance cameras, and highly sophisticated business systems surveilling and supporting the management of complex global supply chains, it is clear we are not far from the broad application of these technologies to military operations. We have the choice of applying AI technologies to improve the functionality and management of the systems and concepts we have today, or we can create wholly new systems and concepts based on those technologies. Our cultural bias takes us in the former direction. This paper attempts to go in the latter direction of new concepts and systems.[11]

AI technologies will be essential to all the concepts I will describe, but it won't be general intelligence; it will be in specific applications of some subset of AI technologies to specific military decision making. Those decisions include: how to maneuver a specific system to best accomplish a mission, reliably making an engagement decision within prescribed parameters, how to maneuver small numbers of systems together to best achieve an operational objective, how to optimally structure and operationally deploy the building blocks of a concept to achieve a higher level military objective, how to best avoid collateral damage and where to place the boundary between an acceptable engagement and an unacceptable one, inference of enemy dispositions and intent from intelligence data, and comparative analysis of potential friendly and enemy courses of action leading to an optimized operations plan, air tasking order or the equivalent in other domains and multiple domains. We are coming to the point where computers will be able to make these decisions, and many others, much more quickly and much more effectively than humans. When we get to the point where all the decisions that have to be made on a platform will be better performed by AI, it's time to seriously consider getting the humans off of the platform.

There is one more fundamental I want to mention before I turn to the central topic of this paper. That topic will become less important as we progress because it can be dropped as irrelevant once one accepts the options that AI and lethal autonomy open up. That fundamental is human behavior and its limitations. Let's start with courage—human acceptance of personal risk. This fundamental has been a constant in warfare since day one. It is embedded in our human "fight or flight" decision making processes. Every military seeks to instill courage—a fighting spirit—the willingness to accept grave risk to self, the warrior ethos, commitment to mission and to the unit, esprit de corps or "elan" as the French once emphasized. Most militaries like to think they have a superior ability to face danger and are better disciplined and more resolute than their opponents. In fact, these differences often, but not always, turn out to be ephemeral or insignificant. Human beings, especially taken in large groups, have a finite amount of courage available to spend. A lot of combat training and military indoctrination is about elevating this level of individual and group

[11] As an aside, I watched the Super Bowl last night, which provoked the following thought. "Money Ball" introduced the idea that statistical analysis could significantly improve results for a professional baseball team. Let's go a step further and apply AI to play calling in football. This is basically a military-like tactical decision about what maneuver scheme to use against an opponent in a given tactical situation. I'm willing to bet that we aren't far from having algorithms that do this better than any coach, and in real time—if they don't exist already.

risk tolerance. Historically units were considered combat ineffective after receiving losses of around 10%. There are many examples of units being effective with higher losses, and some examples of military personnel willingly sacrificing their lives, not just individually but at scale, to attack an enemy (such as kamikaze pilots and terrorist suicide bombers), but this isn't the norm, and I don't think we will ever expect or demand this of Americans. There are also plenty of examples of military organizations that lacked courage, and fled when confronted by their enemy, but on the whole in modern warfare it has not been a major discriminator. As much as militaries have tried to create an advantage in courage through training, selection, and leadership, there is not all that much difference among human beings. As a result, operational analysis has generally ignored this factor, other than to note when units become theoretically ineffective. In theory the willingness to move forward or to stay in place and engage the enemy could be a variable between zero and one. For a machine it could always be one, or whatever conditionally-based value one programs into the machine. While courage is generally not considered a quantifiable variable in analysis of military modernization options, in practice, courage becomes an extremely important factor when comparing manned and unmanned systems and their operational abilities. Machines have infinite courage–again, if that is what is programmed into them, and this fact can be exploited operationally.

The other aspect of human behavior that is worth noting is the inherent limitations of the human body. People must have sleep, food, and water to function, or their capabilities quickly atrophy. Experienced commanders are well aware of the importance of sleep discipline to unit performance. Machines need maintenance, but they do not need sleep. Similarly for the basics of food and water consumption, but in those cases, there are partially analogous needs for energy replenishment for machines. Finally human life support places limitations on design parameters like g-forces, temperature, atmospheric environments, and strength. If we can envision weapons systems without all of these constraints and with military decision making and behavior superior to that of humans, then we should certainly explore that possibility. Which brings us finally to autonomy and the topic the Pentagon currently tries to avoid if at all possible—lethal autonomy. Autonomous lethal systems will be a central focus of this paper. Let's discuss the acceptability of taking this approach.

Lethal Autonomy

Importantly, both modern American "offset" strategies essentially utilized existing force structures and platforms, and simply added new munitions; in one case tactical nuclear weapons and in the other precision munitions. From the point of view of cultural operational change both fit well into existing cultural norms and didn't require fundamentally new roles for operators. The U.S. just used the same or very similar manned platforms to deliver the new munitions to the enemy. Today the emphasis for modernization is on multi-domain operations and JADC2 with ubiquitous high bandwidth connectivity and AI assisted battle command. JADC2 and its Service counterparts also have the feature of overlaying well onto current operational concepts and weapon systems. This isn't a coincidence. I think we can go much further in the next decade or two, but more fundamental changes will be required to do so.

To date, Bob Work's vision of the autonomy-based Third Offset Strategy has not been fully embraced, although experimentation is proceeding across DOD, especially at DARPA. Autonomous functions can reduce the human role in direct combat, and unmanned systems can theoretically largely eliminate it, but there doesn't seem to be any serious consideration of making that transition fully anywhere in the US military. The Military Services are all experimenting with unmanned systems in various roles and fielding experimental prototypes. None, however, have embraced or even seriously considered autonomous lethal unmanned systems as an alternative to manned systems. The closest the Defense Department has come to fielding lethal autonomy would seem to be the use of unmanned air vehicles for reconnaissance and intelligence with very tightly human controlled lethal engagements against terrorists. It can be argued that missiles with various post-launch autonomous target acquisition capabilities cross this line, but the DOD has not considered these systems to fit within the lethal autonomy definition. The US has been very reluctant to explore lethal unmanned concepts, largely because of a strong reticence to accept the consequences and implications of lethal autonomy. There are several dimensions to lethal autonomy, and it's worthwhile to explore them before positing new operational concepts built around the acceptance of at least some degree of lethal autonomy. Let's start with some of the barriers to the use of lethal autonomy and then turn to the potential advantages lethal unmanned systems can provide in terms of the variables discussed above.

When most people think about lethal autonomy, if they think about it at all, they probably have in mind some robotic device with human-like artificial intelligence that may "go rogue" and kill indiscriminately or recklessly. This "Terminator" concept begets an emotional reaction and has motivated a lot of smart prominent people to recommend some kind of an international treaty banning nation states from fielding lethal autonomous systems.[12] In my view, this perspective and this recommendation are inaccurate and impractical respectively. Lethal autonomy in some form has actually been with us for a long time. Lethal autonomy isn't and doesn't need to be human-like in any meaningful way. Here are some examples.

The Improved HAWK medium range air defense system I operated in the 1970s had an "automatic" mode that would have enabled the system, using a truly primitive computer by today's standards, to assess possible threats, apply rules of engagement and fire missiles at threats deemed hostile, all without human intervention. The idea, even in the '70s, was that in a dense air attack situation human operators could not keep up with the decision-making speed required to prioritize and engage individual threats. Almost 50 years later our current air engagement systems are infinitely more sophisticated and capable than the HAWK system I operated in the '70s. Threats are also much more sophisticated in their capacity to work together and employ countermeasures. Human beings still have the same limitations.

A few years ago, I had the opportunity during a trip to Israel to participate in a demonstration of the self-defense capability on a Merkava tank, an active protection system called "Trophy." Once engaged by an operator, the system is highly autonomous. It detects a threat launch at the tank,

[12] The National Security Commission on Artificial Intelligence report argued that the US had to develop lethal autonomy because our adversaries would not be constrained from doing so. I agree with this assessment.

tracks the threat, and commands an engagement with a kinetic kill interceptor that is launched from a container on the tank. All of this has to happen so quickly that human intervention isn't practical. Because this system is defensive, the use of autonomy and the launch of a munition is accepted, although precautions must be taken to protect any infantry or civilians near the tank. There is one other notable feature of this system, however. When Trophy detects a threat, in addition to conducting the intercept of the incoming missile, it also orders the main gun and coaxial machine gun to the point of origin of the threat. There is one more step in that would be needed to automate a lethal response—pulling the trigger. Technically this is a trivial addition to the autonomous capability already in place. There is no real barrier to implementing an autonomous lethal capability, on this or on other weapon systems.

Anti-ship missiles with active and passive seekers that provide for the guidance of the missile to its target have been with us for a long time. Over decades these missiles have become more and more sophisticated. As the range from the launch platform to the target has increased, the need for autonomy has also increased. Ships move, and if one is trying to attack the higher value targets (e.g., aircraft carriers) in a formation of ships with mixed military vessels, commercial shipping, and perhaps decoys, than one needs a smart seeker that can scan the relevant ocean surface and pick out the right target, and even the optimal aim point on that target. Taking this one step further, if the attacker is trying to penetrate layers of soft and hard-kill defenses to get to the high priority targets, it makes sense to share data among the attacking missiles and to automate cooperation to maximize their joint lethal effects. This isn't just lethal autonomy, it is collective lethal autonomy, and to a large degree it already exists.

Given the reality described above, arms control limitations are problematic. As a humanitarian and a human rights attorney, I'm all for effective arms control, but effective means meaningful and enforceable. Given that lethal autonomy is essentially with us now, as the examples above show, I don't see how an effective arms control regime is possible. One has to begin with definitions of the thing one wants to ban. I don't know how to draw a line between the supposedly acceptable types of systems I described above and those that would be banned. Trying to distinguish defensive (good) from offensive (bad) weapons doesn't work when an autonomous air defense system can engage a civilian airliner. Most weapons can be used both defensively and offensively; killing is killing. Trying to distinguish degrees of autonomy is problematic as there is no obvious place to draw a well-defined line between permissible and impermissible technologies or capabilities. The problem here is that there is a great appetite for technologies that automate functions like target detection, enemy intent inference, and optimum engagement planning. These capabilities are continuums with no sharp boundaries. There is a sharp boundary between preparing to engage and actually pulling the trigger but, as with the Israeli Trophy system I observed, that boundary is technically trivial and crossing it would be easy to conceal.

I'd be very willing to engage in a conversation aimed at solving this problem, but I'm not optimistic. One possibility might be to ban all unmanned systems from carrying weapons. This approach would ban existing lethal drones, which one could consider, but it would not solve the problem of the risks associated with lethal autonomy. A system which includes a human operator can still operate in an autonomous mode, like my Improved Hawk air defense system from the

‘70s. It would also tend to ban existing cruise missiles and other fire-and-forget munitions systems with autonomous seeker functionality, something which I expect no major power would accept.

Assuming one could draw a line, there is still the problem of enforcement. The difference between full lethal autonomy and human control is some mechanism by which a human decision must be made to permit an engagement. Think of this as a trigger. In modern electronics systems, a trigger is a switch, which is more likely to be digital than mechanical. It is also likely to be remote from the lethal mechanism itself and the decision communicated through a digital link of some kind. I haven’t heard anyone suggest that it isn’t acceptable to automate everything but the crucial engagement decision. As a result, “cheating” on a ban on lethal autonomy is simplicity itself; somewhere in the weapon system include the capacity to close that switch autonomously. The only way to prevent this from being done covertly is to have extremely detailed design information and extremely intrusive inspection regimes. Even if States were willing to permit this, which they are not, it would be next to impossible to implement.

I would also question whether restricting the availability of lethal autonomy through international law is even wise, assuming it could be done effectively. Is there some good reason why we’d prefer that humans kill and be killed in war as opposed to machines assuming these functions? Over time many unpleasant functions humans performed have been turned over to machines. This includes the mind numbingly repetitive and those involving brute force. A lot of human progress has been about relieving humans of functions that can be done less painfully and more efficiently by machines—freeing humans to engage in other pursuits. It may sound fanciful, but if we have to resolve our conflicts through competitive violence why not let our machines do that for us? This might strike some as ridiculous, but what is really ridiculous to me is that we still have a preference for sending humans out to kill each other to resolve our differences.

I believe there is a better and more pragmatic way to constrain human rights abuses than to ban lethal autonomy; it is to hold the responsible people accountable, regardless of the tools they employ. We have reasonably well-defined laws governing use of force now. The law of war may not be enforced consistently, but it does provide established and agreed limits to the brutality of war and the application of violence. There is no reason why the people who unleash indiscriminate autonomous killers on innocent victims including neutrals and non-combatants cannot be held accountable for their behavior. At the end of the day, we want to constrain the behaviors that we find objectionable. I believe we can still do that without banning autonomous weapons.

It would certainly take some effort by legal theoreticians and others to determine who in the chain of control of an autonomous lethal system to hold accountable and what the standards for violations should be for specific acts. I would offer that a good place to start is by enhancing the standards that we apply today. Currently, we accept that some “collateral damage” is inevitable in war. We ban collateral damage that is not a military necessity, intended to inflict terror on civilian populations, or intended to achieve genocide or ethnic cleansing. If we are going to permit autonomous machines to make decisions about lethal engagement, shouldn’t we raise the bar for when that’s acceptable? In any event, the minimum is the standard we employ today, and there is no reason to relax it. Who should be held responsible? This is a matter that is very standard in

criminal law and personal injury cases; determining intent or degree of negligence required for liability. Any person or State that uses an autonomous lethal system should have a legal duty to ensure that system will not violate the laws of war. This means that the designers, the testers, the acquirers, the fielders, the military operators, and the political decision makers, all have a duty to ensure that a fielded system is compliant with established rules governing operational behaviors. In some cases, strict liability could be implemented. It might be useful to also require that a specific designated official and organization be responsible for testing and verifying compliance, analogous perhaps to air worthiness certification today. For egregious violations—the intentional wholesale slaughter of innocents—the humans who directed or even permitted this use would be responsible, just as they are today.

As a last point on this topic, I don't think the development of lethal autonomy can be stopped or even slowed appreciably. Most of the enabling technologies will proceed for independent reasons. The military advantages of employing lethal autonomous systems will become increasingly apparent to all. As I look at just ongoing US military service and DARPA efforts in this area, it is clear advances that will take us right up to the edge of lethal autonomy are well underway and advancing rapidly. Some nation states and groups will not hesitate to embrace this opportunity, regardless of any ethical concerns. I've heard representatives of several liberal democracies state publicly they will pursue the relevant technologies because of the fear less principled States will do so. Almost daily I read open literature accounts about new unmanned lethal systems or improvements in the relevant areas of artificial intelligence—especially pattern (target) recognition. This genie will not be put back in the bottle, so let's open the bottle and see what might be inside.

If one can get past the objections to lethal autonomy, it opens up a fascinating range of options, including tactical behaviors that would certainly not be doctrinal for manned systems. Specifically, it is generally permissible to sacrifice unmanned systems, singly or in groups, for a tactical or operational advantage. My friend, retired Army MG Bob Scales, likes to talk about how a fundamental function of infantrymen, particularly in counterinsurgency campaigns, is to walk down a trail with a rifle toward the enemy in order to draw fire and expose the enemy to attack. That's an oversimplification, but there is some truth in it. I once convened a group of general officers in the Pentagon to try exploring ways to end this paradigm. We didn't get very far, but the option of using relatively inexpensive and expendable unmanned systems for this purpose is very attractive to me.

Common Conceptual Threads: The Relationship Between Projectiles, Launchers, and Transporters and A Key Role for Humans

I started to write this section with the hope that across domains there was a common way to describe weapons systems and operational concept components, and a common way to talk about an optimization paradigm. My thought was that there might be a common solution conceptually at least in the trade between projectile range and cost, the number of projectiles in a launcher and its cost, and the capacity and cost of a launcher's transporter (where one was required). I was thinking

of the arsenal plane or arsenal ship concepts and an Unmanned Ground Vehicle (UGV) carrier concept that would all be attractive solutions so the world of unmanned lethal autonomy warfare operational concepts in one domain would have similarities to other domains. After some effort I couldn't convince myself this was clearly the case, but it still seemed a useful way to discuss concepts in most domains. Also, while there is commonality in the implications of some key parameters, each domain brings its own unique characteristics. In particular it is easier to survive in some domains than others, so one can venture closer to the enemy with larger, more expensive platforms. It is also easier to communicate in some domains than others, affecting the ability to use off board sensors, to fuse information and to coordinate platforms and weapons. While the tentative domain-specific concepts I will suggest may not be similar, the concept of projectiles, launchers and transporters has validity, and most domains can be approached from that perspective. Alas, warfare is complicated and there is no avoiding the complexity of the specific design trades involved, but there is at least a common way to approach or think about the problem.

As I worked my way through thinking about and writing about each domain and multi-domain operations, one common concept that did emerge was in the role of humans. In every case, I found a need to include humans at an organizational level somewhere above individual engagement decisions and small unit tactical behaviors, but not far above those levels. My view was that humans would be needed to control operations at that level; they are needed to provide an executive decision-making function for force management. At this level, time constraints are in my opinion less severe, making processes at human information processing and decision-making speeds operationally acceptable. I do envision robust AI-based decision support tools at this level, but not complete autonomy. Against responsive threats and in a broad range of operational contexts, something closer to the general intelligence humans have is needed to at least oversee operational decision making. I don't expect AI to provide that any time soon.

In the balance of this paper, I will be discussing various warfare domains. In all domains, warfare is largely about applying destructive force to something one wants to destroy without being destroyed in the process. Simply and abstractly energy must be delivered by a "projectile" to a target to kill that target. Something, a "launcher," provides the deployment mechanism for the projectiles. Another object, a "transporter," may be necessary to move launchers to where they can be employed. This can be a useful construct because so many of the design trades involved in a concept are about the balance of fundamental features among these elements. The range of the projectile and the payload it carries (warhead and guidance for example) drive its mass and other characteristics. The projectile mass and dimensions drive the launchers payload capacity, as does the stowed inventory and the range of the launcher. If a transporter is involved (aircraft carrier for example), that platform in turn is constrained and dictated by the mass and dimensions of the launchers and stowed projectiles the transporter must bring within range of the launchers. Obviously, the laws of physics constrain everything, as do a number of other factors, and sometimes there are more, or fewer nested entities involved than two or three. Everything in a concept of operations can't be shoehorned into this model, but it's a useful place to start when, as here, one is working with a clean sheet of paper.

The fundamental objective is to apply energy to an enemy target and destroy or neutralize that target. That energy is delivered by some form of a projectile—which can be a bullet, a missile, a torpedo, or the photons in a laser beam, as examples. Projectiles are consumed in use, so they need to be cheap. We'd also like them to be long-range, resilient, and have high kill probabilities, all of which adds costs of course. Projectiles are never manned, even today. These projectiles are sent on their way to the target by some sort of device we can call a launcher. I'm thinking of a launcher as a platform, not just the launching device on a platform. Today this can be a tank with a main-gun, a tactical aircraft with internal or wing-mounted launch points, or a surface ship from which the projectile—the bullet or missile—originates. Launchers may or may not be reusable, and they may or may not be manned. In my concepts they generally will not be manned. If launchers are not reusable, we want them to be very cheap. If reusable they need to be survivable through some combination of stand-off range and other features—which again adds cost. Since we are assuming unmanned launch platforms, we can also talk about attrition being more acceptable, so there is a more open design trade-space than we would consider for manned systems. Finally, the launcher has to be delivered to a place where it can be utilized so that the associated projectiles can be affective against the targets of interest. We can call that device a transporter. Some launchers double as transporters—they self-deploy, at least to some degree. Others have to be moved to within ranges where they can operate tactically. This can be done through pre-positioning, such as on forward airbases, in pre-positioned depots, on bases close to the expected area of operations with locations dictated by the operational range of the launchers, or by transporters like aircraft carriers, surface ships, trains, and trucks. I will make some judgements, valid or not, about the threats to and the survivability and resilience of the transporters, but like it or not they are necessary and have to be considered a part of the operational concept. Because the United States' conventional forces are intended for power projection applications thousands of miles from our shores, we have a particular requirement to consider how we will get to, or already be, located where the fight will occur.

This hierarchical system can be thought of as a nested set of systems. An aircraft carrier is a transporter. It brings launcher airplanes to where they can reach close enough to the enemy targets that the projectiles carried by the airplanes can reach the targets of interest. Historically we rarely if ever design all the elements of this suite of systems at once so that they can be optimized relative to one another. We are almost always trapped by the existence of large prior capital investments that constrain us. The new missile has to be compatible with the existing aircraft, the new aircraft has to be compatible with the existing aircraft carrier and the existing missiles—and on and on. We should take advantage of the opportunity autonomy and other emerging technologies give us to rethink the entire design or our future warfighting concepts. We ultimately may not completely break free of our past investments, but we should at least start our thinking and analysis unconstrained by past decisions.

One of the limiting factors in the existing nested projectile/launcher/transporter designs has also been the need to include human beings on the transporters and launchers, for a wide array of functions. A tank is a good example. If the functions of driver, gunner, loader, and commander have to be performed by humans, the tank design must incorporate protected volume for these

people together with the tools they need to do their functions and the supplies they need as human beings. In addition, the launcher has to accommodate weapons (main gun and auxiliary weaponry) and a reasonable number of projectiles. As we automate the functions of the crew, we can eliminate some of these constraints incrementally. If we eliminate the crew entirely, we can reimagine the whole trade-space as well as the range of possible tactics and operational techniques. In every domain, the projectile, launcher, and transporter trade-space can move to a new optimal design point. We can at least approach the problem in each domain by thinking about the trades between these functions.

We can start this process with a known entity. The amount of energy it takes to defeat a given target is fairly well understood. The projectile's job is to get that energy to the target. That energy is the minimum payload our projectile has to carry. The other feature that sizes the projectile (think missile) is its range. The farther we want the projectile to travel the bigger it will be and the more expensive it will be. Because projectiles are generally not reusable, once they are sent, they are expended.[13] Things we will consume instead of reuse should be as cheap as possible. Therefore, we would like the launcher and carriers to be able to get close to the targets so that we can use short-range weapons and carry more of them per reusable carrier. Unfortunately, it's not quite this simple; projectile range also adds targeting flexibility, which has value, and improves the survivability of the launcher, so there is some appetite for projectile range. We also want as many projectiles as possible to arrive at their targets successfully, so there is a cost to complexity optimization trade to balance the numbers of projectiles needed and the probability any given projectile gets to the target to minimize the total cost per kill. Hypersonic weapons are a good example of trading high cost for high probability of successful penetration to the target and hopefully successful target engagement. Moving up the chain from the projectile to the launcher to the transporter we can start to define concepts that have some relevance for each domain.

Many current ideas for autonomous unmanned weapons systems fail to consider the need to get those weapons (launchers and projectiles) to where they can be useful; how are they transported to the operational area in a survivable, reliable, timely, and cost-effective way? If pre-deployed, are our assets survivable against surprise or warned attack? If not, how will we get them where they need to be? If we are assuming high rates of consumption or attrition for projectiles and launchers, how will our losses be replaced over even a moderately protracted conflict? The trade-space for weapon systems design, and for operational concept design, involves all three of these functions with many possible variations and combinations other than the simple three-part harmony just described (projectile, launcher, and transporter). This trade space manifests itself in decisions about how many projectiles on what types of launchers and what type and capacity of associated transporters (if any) are needed to complete and to optimize overall cost effectiveness. We can certainly combine these functions, and we don't need to be limited to only three components.

[13] Conceivably projectiles that can't find acceptable targets could return, be refueled, and be reused, but the cost of including this in a projectile design is likely only justified if a large fraction of the projectiles will not find and attack targets.

In the concepts for each domain, we also of course have to provide for other necessary functions besides delivering lethal energy to targets of interest. These include surveillance and targeting, battle management, communications, command and control, and especially sustainment. I will touch on these topics, and other domain specific complexities in the sections that follow.

Sustainment, in particular, is a major cost driver and often neglected when operational concepts are considered. Relying on autonomy opens up new options and creates challenges for sustainment. Consider either sustainment model (American or Soviet) discussed earlier as compared to one that would be possible if the vast majority of our fighting platforms were unmanned. We would need to use some fraction of these platforms in peace time for experimentation and to train the AI tactical software that controlled them, but this could all be accomplished with a small number of platforms; most of our assets could be idle and not undergoing the wear and tear of frequent or continuous training. Upgrades could be done much more efficiently. Software changes (most functionality will be software-defined in the future) could be done across the force very quickly. Hardware upgrades, which would be substantially less frequent, could also be scheduled much more efficiently because we wouldn't need to schedule around human training cycles and deployments. As indicated above, at some level of the force structure, there would still be operators whose role would be to manage, oversee, and control the autonomous platforms and the small units composed of autonomous platforms, but this would be done remotely from a small number of platforms or command and control nodes. Realistic simulations, anchored by constant experimentation, based on field experience data, would provide a fully adequate low-cost training environment for these operational executive level people. The benefits to peacetime cost and reduction in support structure would be enormous. There is a valid engineering trade-space between sustainment related design features, cost, and operational effectiveness that would be opened up by reliance on unmanned autonomous systems. The optimum design choices would take into account wartime expected life and design for fairly high reliability after long periods of storage and inactivity. So called "wooden round" munitions have been designed for highly reliable shelf life for some time, but less stringent requirements would probably be adequate, even optimal, for more expendable unmanned fighting platforms (launchers and transporters)—especially if most faults were detectable autonomously with high confidence at system "start-up." Life cycle costs, and both peacetime and wartime sustainment requirements have to be part of the trade-space.

Responsive Threats and Enduring Advantages

It should also be noted that every innovative military development provokes a response. Introduction of the new model forces I'll describe in the following sections would cause a strong and immediate reaction. There are three common responses to innovation on the battlefield: rapid reaction, deliberate countermeasures, and emulation. A good recent example of the US responding to a new threat was the introduction of improvised lethal small UAVs at scale by ISIS against the Iraqi Army and US Special Operators in 2015 and 2016. The first phase of a reaction would be similar to that of the US, a rapid acquisition program and responsive tactics to address the new threat. For the ISIS UAS problem this took the form of the rapid introduction of urgently procured soft and hard-kill small UAV defeat mechanisms into the force, even if limited in their

effectiveness and overly expensive. This is followed by a more thoughtful and sophisticated approach which may include novel and new designs. In the counter UAS case, examples of this included research on special purpose smart proximity rounds, purpose-built target acquisition and fire control systems for existing guns, high energy lasers, and area weapons employing high power micro-wave engagements. These responses in turn lead to more sophisticated small UAV threats—with some combination of hardening, deception, and counter-kill.[14] More significantly they lead to emulation—the adoption and extension by others of the new technology and operational concepts, such as the widespread adoption of small armed UASs, which we are seeing today and which I discuss as part of the concepts I will describe in this paper. This in turn leads to a period of incremental improvements on all sides until eventually a new revolutionary concept is enabled by emerging technology and operational innovation.

As technology changes warfare, advantages can have varying degrees of longevity. Some changes will be emulated immediately, with lead times measured in months or at most a few years. To the extent the technologies involved are militarily unique and difficult to copy, advantages can be of longer duration. The recent example of the U.S. advantage in precision munitions, stealth, and wide area surveillance had a relatively long life, arguably about two decades, before the same technologies were adopted successfully to be used against the U.S. Stealth has been particularly enduring. What these technologies have in common is that they are military technologies with little or no commercial applications. The greater the depth of knowledge required and the more specialized the technology, the longer an advantage based on it lasts. It's comparatively easy to control access to the militarily unique technologies because they can be kept concealed during development and are harder to emulate or reverse engineer once revealed. Even for these technologies, the most important piece of information—that they exist—cannot be concealed for long. It's easy to focus research and espionage efforts once an existence proof has been provided by an adversary. Consider, for example, how long the U.S. nuclear monopoly lasted. The technologies that form the basis for this paper, on the other hand, such as those associated with autonomy, some of the artificial intelligence technologies, and modern information systems technologies are all commercially based and will be widely available. Any advantages obtained from them will be relatively short lived and they will lead to more militarized versions of those technologies very quickly. The game goes on, and as long as humans chose to resolve their differences by violence, it never ends.

Domains of Warfare and Multi-Domain Warfare

At last, we come to the heart of the matter; what will future warfighting operational concepts consist of and what systems will be included in them. There are no clean domain boundaries, and one can argue endlessly about definitions. The intent here is to be pragmatic, not tautologically pure. In addition to land and air domains, I've divided sea into surface and subsurface. I've also

[14] This is a good example of why commercial products don't have long operational lives. Once the adversary starts finding ways to attack the commercial products, (for example through jamming, cyber, and directed energy) the militarily unique requirements start to pile up, and before long the commercial product is replaced by something much more highly specialized.

added space and cyber as domains. I did not add the electromagnetic spectrum or EW as a separate domain but chose to handle that in the context of the other domains.[15] Cyber is discussed both in the context of each domain and as a domain in its own right. My logic was to think of domains as abstract "terrain" on which forces were organized and equipped at scale to contest for control of that "terrain." In each case the physics of the "terrain" has features that are major drivers for the forces involved. It's easy to quibble about these choices. I was looking for a reasonable organizing structure, not a definitive correct answer. Readers are asked to accept, if only for the purpose of this paper, that the chosen list of domains is a reasonable basis upon which to lay out some concepts and ideas for the future of warfare. I will discuss multi-domain implications in each section, and I have included a section dedicated to multi-domain, Joint, and Combined operations at the end of discussion of the individual domains.

For each domain I'll provide a short introduction, discuss the operational concept I envision and the building block components of the concept. I'll then cover a list of complexities associated with each domain. The lists tend to be long; warfare is complicated. I've organized the so-called complexities somewhat arbitrarily by three categories: (1) fundamental operational needs, (2) design requirements and considerations, and (3) other needed military functions. Within each category, topics are arranged alphabetically. For each domain, I include cross domain considerations under fundamental operational needs and responsive threats under design requirements and considerations. We should expect and even demand significant cross domain functionality. All domains will have cross domain complexities; they will take the form of cross domain dependencies, support, and effects. There is also great virtue in military concepts in having redundant ways to do anything; redundancy provides flexibility, enables surprise, eliminates single points of failure, improves resiliency in general, and compounds the enemy's problem dramatically. Each domain will also have complexities unique to that domain.

Throughout all of this, the design trades are complex and have to be done in detail in each domain to reach anything like optimal results. All I can do here is lay out some intuitively interesting possibilities, anchored in a lifetime of work on the intersection of technology, military systems, and innovation. If we discard our preconceived notions about what platforms and weapons should look like, and embrace the potential for widespread use of autonomy, we will enter a brave new world of conceptual design. I can only begin to explore that world here, but we can think constructively about the possibilities and lay the groundwork for more quantitative analysis. Let's get started.

[15] There is an ongoing debate about this that I don't have strong feelings about either way. Control of the electromagnetic spectrum is hugely important to warfare in virtually all domains, undersea being up to a point an exception. What's important is understanding EW's significance and potential decisiveness in any domain and that it cannot be separated from considerations about how to prevail in each domain or the need for action on that knowledge.

Warfare Domains – Land

Introduction

Land warfare is about taking and holding ground. It is the oldest form of human warfare and has continuously evolved. That evolution has been driven by changes in weapon range and lethality, degrees of protection against those weapons, and mobility. Mechanisms for acquiring information, command and control, and logistics related technology have played important roles as well. The ground environment provides natural protection, both cover and concealment, restricts movement, and limits lines of observation and fire. Urban environments are especially close and complex, leading to high casualties. Ground combat has always been intensely dense with human participation and direct action between human combatants, and casualties at the point of contact tend to be very high. I believe in the not-too-distant future, while the environment and its implications will remain, the direct participation of humans will decrease dramatically.

Operational Concept

As in other domains to come, we will start with a blank page. There are no "squads" of infantry soldiers or "platoons" of manned armored vehicles. Those concepts are going to be untenable. Humans are too valuable, too expensive, too targetable, too slow, too vulnerable, and not capable enough to survive in combat against the types of forces and formations envisioned here. Because of its relative complexity, the land combat domain is the hardest domain in which to make lethal autonomous forces practical, but it is going to happen. Fundamentally we need three technology-based capabilities, all of which are more difficult in this domain than others. They are autonomous mobility, autonomous small unit tactical behaviors, and high confidence target acquisition. I've watched all of these technologies mature over many years, and I believe we are close enough in reach now that this is a realistically foreseeable capability. What I will describe is an operational concept, a new model force that completely dominates current conventional ground forces. The force envisioned can conduct either offensive or defensive operations, but it is especially effective at defeating maneuvering conventional forces, mechanized or infantry. I will describe how this force operates to defeat a conventional modern human-centric force.

The basic concept is an echeloned force that combines ground and airborne unmanned autonomous systems operating in conjunction and in teams, with a nested command/management structure that is very adaptable, tailorable, and dynamic. At the lowest levels, where tactical engagements occur, decision making is highly automated based on rules of engagement and temporal and spatial constraints. As one moves up to higher levels of force size and integration, human decision-making is introduced as it becomes more necessary and effective. The volume of information flowing from lower to higher echelons is minimized and tailored to that needed to support the decisions best made at a higher level of aggregation. In any many-on-many dense scenarios, this would not include the highly detailed information to support individual engagement decisions by humans, or even to support small unit tactical decisions by humans. It would initially include information to support force management decisions and operational scheme of maneuver decisions, but even

lower echelon (think small unit at least) decisions in these areas could be largely automated. This structure can also learn autonomously at each echelon level and adjust both tactics and organizational structures in near real time in response to threat situational awareness and observed threat behaviors.

Within the new ground force model, medium sized armed airborne systems (launchers) with vertical take-off and landing capability are launched from a ground "mother-vehicle" (tactical transporters) which contains multiple, possibly stacked, vehicles that provide lethal effects, target detection and identification, and participate in cooperative distributed tactical decision making at the lowest echelon level. The airborne systems operate collaboratively in small units (nominally say four air vehicles launched from the same ground vehicle). The lowest echelon size is flexible, but it could be anything from two air vehicles to say ten. The air systems provide airborne line of sight engagement capability and autonomous ground systems provide primarily indirect fire capability and ground transportation, energy, and munitions reload support to the unmanned aerial systems. Multiple ground vehicle configurations would probably be necessary to keep the individual ground vehicle sizes optimal. Different configurations could include indirect fires (launcher/transporter role) and air vehicle transport and support. One configuration could be a direct fire capability, and all UGVs might have a minimum self-defense capability in order to provide resiliency. I'd categorize both of these air and ground vehicles as attritable. Manned C2 vehicles would be designed to be more survivable, mostly through stealth, and employ tactics to avoid being engaged.

Above the first echelon level would be higher aggregations of organization and automated behaviors, using the lowest echelon as behavioral organizational building blocks. The analogy to squads as the lowest level followed by platoons and companies, all with similar organic capabilities is reasonably valid as a starting point to visualize this, but the model force does not have this rigidity. Tactical behavior models that would be automated would extend two, three or more echelons above the lowest echelon. The force model includes an automated or semi-automated hierarchical C3 Battle Management system at each echelon that directs both the organizational structure, and the employment of the echeloned forces assigned to operate under its control as a unit. Again, the analogy to current echeloned operational planning is apt, except that in this case it is much more flexible, automated, and tactically optimized to suit the immediate operational situation.

The intent of this structure is to overwhelm and destroy an opposing mechanized or infantry force in any given assigned area of terrain with highly favorable cost exchange ratios. Swarming does not capture the intent. The idea here is more sophisticated and threat responsive, although there would be some similarities. At the lowest tactical level, small numbers (nominally 5 to 10) of airborne systems would scour an area of interest and depending on the results choose an operational mode most efficient for destroying an enemy force or targets in the area. This function would be used in an offensive, defensive, or movement to contact mode as dictated by the mission. Specifics of tactical behaviors and resource management would vary depending on the situation, however.

The preferred engagement in this concept is by indirect fires or UAV direct fire (which could be just-beyond-line-of-sight). I have made some provision for direct fire capability on ground vehicles above for resiliency, but the basic idea is that individual or ground vehicle-based line-of-sight-fires have gone the way of hand-to-hand combat; in this concept those engagements are not quite obsolete, but they are not preferred, rarely occur, and are avoided if possible.

For a conventional opposing human centric infantry and armor force of any type, direct fire engagements from the medium UASs would be one available option as would be coordinated indirect fires from ground platforms within a few kilometers but beyond line of sight of the opposing force. The air vehicles in the concept would support indirect fires with targeting quality information. Target identification would normally be an organic capability of the air vehicles within established rules of engagement and confidence levels, minimizing time delays and communications loads. In some lower intensity situations dual redundant target ID, and/or other safeguards, could be mandated to reduce false positives. The force would seek to optimize the mix of weapons and the exposure of air vehicles to enemy lethal mechanisms in order to be most cost effective at each echelon. The immediate operational depth achievable at the lowest echelon by the organic air vehicles would be a few kilometers. The endurance of the air vehicles in the concept would be consistent with operations at that depth. Ground vehicles would have range and endurance characteristics to support operations over something on the order of 200 kilometers or more.

The concept described would replace current maneuver forces. Additional ground forces would probably still be needed to provide operational depth, including long-range fires and extended range surveillance. I say probably, because it isn't clear to me how much of these functions could be off-loaded to space and airborne forces. If they are still necessary, physics would dictate larger platforms and longer ranges for the components of the extended range suite of capabilities. There are strong efficiency and total force resiliency arguments for the inclusion of long-range ground launched munitions and the supporting C3BM and target acquisition capabilities necessary to support them. The challenges to automating these functions are arguably less than for the maneuver and close combat functions, however.

As indicated earlier the concept would be incomplete without consideration of sustainment capabilities. The force I have described is not a throwaway expendable force. It does have an operational virtue that some systems can be sacrificed to find the enemy, to force him to engage, or as part of a deception. These behaviors should be part of the automated and semi-automated suites of tactical behaviors, but the air and ground vehicles I have described are going to be sophisticated enough and costly enough that they should be reused over multiple missions or operations and therefore have to be supported. The air and ground vehicles would be medium sized and tactically self-deployable, together and separately, but they would need transporters to bring them into an operational area.

If we apply the projectile, launcher, and transporter concept described above, it looks something like this: The line-of-sight projectiles are fairly conventional—small missiles, grenades, or bullets. It's necessary to have the engagement capability for a variety of targets, so suitable mixes of

munitions are needed. To the extent flexibility to carry different projectile types can be designed in, it should be incorporated into the UAS launchers/transporters. The launchers are the UASs and UGSs in the concept. UGSs also serve as tactical transporters for the UASs. Each UAS should be able to carry one to 10 stowed munitions depending on the target type. The air vehicles I have described will be transported on the ground vehicles. Depending on their form of propulsion (battery, liquid fuel, or fuel cell) and weapons load they will need to have their energy source replenished and potentially weapons replenished from the ground vehicles. The ground vehicles will deliver themselves forward after transport by a larger class of system in some non-tactical mode—air, rail, road, sea, or a combination thereof. Ground vehicles could be resupplied forward autonomously or self-recover to a more centralized refueling and rearming point. There would be no organic maintenance capability. Mission incapable ground vehicles would self-evacuate if able or be towed from the operational area by other ground vehicles if salvageable. In some cases, air vehicles could also self-evacuate. As in other areas, there are trade studies that would have to be conducted to optimize the level of investment in repair capacity and where or if it should occur, but repairing forward is not intended.

Human command and control would begin at a level roughly equivalent to Battalion or possibly Brigade. Lower echelon engagements would be monitored at this level but not tightly controlled unless by exception. The organizational concept is intended to be largely self-sufficient. The tactical echelons described can conduct ISR locally, plan maneuver and engagements, and manage operations as they unfold. Provision will be made to provide off board support including intelligence, targeting, and supporting fires from higher echelons and other domains, but outside support is not a critical operational dependency. C2 would be distributed, with each echelon's UGSs capable of managing the units or platforms currently assigned and a small group of UASs acting as a team would self-manage as a team. Dedicated manned C2 vehicles would be introduced at battalion or brigade level. These vehicles would be designed for improved survivability based on deception and concealment primarily, and they would be able to operate several kilometers away from the balance of the automated force. Organic airborne communications relay systems using dedicated UASs are likely to be required as a result.

Building Blocks

Small to medium UASs will be rotary wing vertical take-off and landing from UGVs and have operational ranges and endurances consistent with missions of one to four hours and payloads of 10 to 100 pounds for munitions (one of many trade studies needed) in addition to organic sensing, navigation, computing and communications capacity. An alternative worth analyzing is to distinguish ISR UASs from weapons carriers. At a minimum, the idea of using some common UASs with no weapons loadout as dedicated ISR platforms for a given mission should be considered. Projectiles carried by and launched from UASs would be relatively short-range to reduce weight and cost. The UASs would be hardened against EW and cyber threats and be able to operate in a reasonable range of weather conditions. They would be compatible with ground vehicle transport and servicing for energy and expendable resupply. Growth capacity for survivability features would be desirable. They will be able to engage manned helicopters and

some UASs in a sacrificial mode of attack at least. UASs and the more capable projectiles carried by them would be mass produced using commercially-based components and processes with nominal unit cost on the order of $10,000 or less.

Autonomous ground vehicles will function as UAS transporters and support vehicles and indirect fire launchers. They would provide cost effective operational movement on the battlefield. They would generally be wheeled with roughly the mass and form factor of a medium-sized pickup truck. They would be mass produced with modular mission packages—especially UAS transporters and indirect fire launchers. Tactical indirect fire variants will carry weapons with medium range (out to say 10 or 20 kilometer) engagements. All variants may carry a limited self-defense direct fire system, with small UAS engagement capability, and line of sight sensors, generally passive. Although the UASs are the preferred direct fire engagement systems of the concept, the UGVs may have a tactical capability beyond self-defense. They can be networked locally and programmed for collective tactical action in small numbers. Ideally, the UGSs and UASs should be able to operate together tactically in a combined arms direct fire assault or final protection mode, but this would probably not be the norm. The trade space for these platforms balances cost, range, protection levels, weapons capacity, and sensor and communications payloads with a strong emphasis on cost. As UASs, weapons and fuel are exhausted, UGS vehicles can autonomously redeploy to rearm and refuel or recharge.

Local information systems or architectures, which include communications, sensing, processing, and data storage are the heart of the concept. Together they must constitute a balanced design that is resilient and hardened against attack. Processing and data storage should be pushed to the edge of the architecture to minimize the burden on the communication links and to support as much platform and lower echelon level autonomy as possible. Most architectures being designed in DOD today are in my view too centralized and are intended to support a heavily human supervised or human decision-making function. Commercial technologies will be important to this architecture, but military requirements will exceed and be very distinct from commercial capabilities. Collaborative sensing and tactical decision making based on AI will occur and be automated, but primarily at the tactical edge, empowering individual platforms and small collections of platforms organized virtually to collaborate. Above this level the focus will be on higher echelon planning and force management based on reasonable aggregated and processed data provided by lower echelons.

Complexities

Fundamental Operational Needs

Command, Control, and Communications (C3): Any unmanned system intensive concept is highly dependent on resilient and effective C3. I've discussed this in part earlier, but it's worth some additional comments. The C3 architecture is the great enabler for all the concepts, but it's especially important for the ground domain due to terrain effects on communications links and the need to form ad hoc operational networks, as well as the sheer numbers of participants, the need to deconflict them, the proximity of jamming threats, and the amount of information that has to

move on the network at scale. In the commercial world, 5 G is the emerging state-of-the-art and 6 G is in early stages of development, but there may be limited direct application of these technologies to ground operations. Military C3 networks are particularly challenging for several reasons, and I don't believe there is a network today that can support the concept I've described in a contested environment. I do believe, however, such a network is obtainable. Achieving that will require careful design of the information flow the network has to support and of features unique to military systems. There will also have to be well developed options for reduced performance under stress down to some operationally viable minimum product level. As a design principle, I believe as much processing as possible should be conducted at the tactical edge, generally on platforms that carry surveillance sensors as payloads. The target identification function described above should happen at the sensing platform level so that only target classification, confidence level, and tracking information is passed to more centralized nodes for fusion. The DOD has tried in the past to create architectures in which much more information is shared among platforms and passed to higher echelons, often with the goal of real-time human interaction with fused imagery. If we start with that goal, this problem may be intractable. If we start with something much less ambitious, but still operationally transformative, I think we can get there.

Extended Range Precision Fires Including Hypersonic Weapons: The concept focuses on relatively short-range engagements and continuous control of the tactical battlespace. It does provide for automated longer-range systems but the cost per kill of those systems is expected to be higher than the UAS-carried munitions, and they don't have the same enduring and robust control over terrain. They do have the ability to mass fires, but the UAS systems have that capability also, although less responsively. A trade-off to balance these capabilities would be needed. Traditionally artillery has been the most cost-effective weapon in ground combat because of its flexibility, accuracy, and low latency and cost, but the advent of the UASs described creates a new balance that should be analyzed. Precision munitions (missiles or shells) significantly enhance the effectiveness of artillery. The need for ground launched hypersonic weapons isn't as clear to me. They have faster time on target but are expensive and may not be able to engage mobile ground targets effectively. The concept does not depend on them and their cost effectiveness should be investigated—it isn't obvious to me.

Logistical Support—Expendables and Consumables, Infrastructure, Supply, Repair: Some of this was covered above in the description of the concept. The logistics concept for the whole force should be designed, at least to first order, as a next stop in fleshing out the concept I've described. An unsupportable force isn't a force. It isn't well known, or advertised by the Army, but most of the Army, by a wide margin is trucks, not combat vehicles. There are many tens of thousands of trucks in the Army (over 100,000 HMMWVs alone) and only a few thousand combat vehicles. This concept could fundamentally change that ratio, but there have to be provisions to flow fuel and ammo and the items necessary to support the humans in the concept forward to where they are needed, both by ground and by air. This could be accomplished largely with automated unmanned systems (possibly commercial platforms), with special automated handling equipment compatible with the manned and unmanned receiving platforms. The dramatic reduction in numbers of humans in the concept should relieve many current logistics requirements, but each of those

functions (medical, graves registration, personnel replacement processing, detainee and refugee processing, etc.) still have to be considered and provided for in the force, even if to lower numbers. The provisions I described above were intended to automate as much of the logistics function forward as possible—no organic maintenance personnel, self or sister vehicle platform evacuation, automated rearming and refueling, for example. Some operational attrition of the force due to logistics shortfalls may be acceptable, but it shouldn't be widespread. Logistics cannot be an Achilles heel of the concept. Modular designs would make automated intermediate level repair in the form of module exchange more tractable. In this and any future concept, AI based support functions, including proactive prescriptive maintenance/evacuation and inventory management should be part of the design trade-space. As in the kill chain approach to engagement analysis, the whole logistics chain has to be analyzed and optimized as part of the concept.

Multi-Domain Considerations: The ground domain concept described above is built around an operational force that is designed to take and hold ground. It includes UASs designed to support that mission. I didn't let the fact they are aircraft constrain the concept; their role is primarily to find and attack ground targets in support of ground operations. Forces from other domains can also attack ground targets. For the future ground concept, and all others, relevant information to support operations will come from other domains, in this case primarily air and space systems. Fires can also be provided from other domains, especially the air domain in this case. In addition, support functions such as transportation, communications, PNT, EW and Cyber support will all come from other domains. Finally cross domain support can surveil, target, and engage threats of high priority to success in the ground domain. Those enemy targets include enemy command and control, surveillance systems in any domain, but especially space and air and systems that provide the enemy with long-range precision fire capacity. The design challenge is to optimize this cross-domain collection of capabilities and to simultaneously make it resilient enough in the face of enemy attack to be successful.

Tactical Mission Variations (scouting, hasty and deliberate offense or defense, and movement to contact, for example): These missions would still exist, and the concept has to accommodate them. I don't see anything prohibitive about applying the concept to address these and other missions through a number of essentially templated and automatable Tactics, Techniques, and Procedures (TTPs) associated with each mission. The availability of infinitely tailorable tactical organizations, without regard for unit cohesion, provides enormous flexibility. This is one place where human decision making would be useful, at least initially, in defining missions for tailored "units" of unmanned systems. What should be automated are the decisions about tactical behaviors at the small unit level and individual platform level within an assigned mission. As the concept matures, more sophisticated and higher level automated tactical and operational decisions should be possible, but that isn't necessary at the outset. Even at early stages, AI can support human decision making about courses of action.

Target Identification/Collateral Damage Avoidance: This is the core enabling technology for lethal autonomy. It has to be at least as good, and probably demonstrably better, than human decision making in the same situation. This is a measurable activity that can be tested in simulation and in the field. It is also a capability that can be traded operationally in real time by adjusting decision

algorithms to improve performance or react to changed conditions (the appearance of a large number of civilian refugees in an area for example, or conversely the indications of a major enemy advance through an area). Human monitoring and override authority would be part of the concept. In less intense environments with more time available for decision making, human control of engagements could be exercised.

Design Requirements and Considerations

Civilian Engagement and Interaction: It will happen, and the autonomous behaviors, especially by the ground vehicles in the concept, will have to accommodate the range of interactions. The range includes friendly, neutral, and adversarial as well as both individuals and groups. When the force is operating among potentially hostile civilians, provisions may have to be designed-in to effect a range of responses and there would need to be a way to communicate with civilians to reduce risk and manage any given situation. Moving—or not—through hostile protestors comes to mind. What to do about children throwing grenades comes to mind. This is one place where human remote involvement or control might be necessary. The default in some cases would be to avoid injury to humans completely, in others to sacrifice the vehicle, and in others it might be a lethal response. What it may come down to is the force defined in this ground domain concept and designed to defeat a conventional armed ground force at scale, isn't suited to the human intensive environment of a counterinsurgency or counterterrorism mission. That said, the elements of this concept could still be very useful in such an environment.

Confidence in Automated Behaviors: It can never be perfect, but a number of constraints can be in place to prevent mistakes. These would include temporal and spatial boundaries on movement and/or fires, the requirement to seek human permission if certain thresholds are reached (such as the numbers of engagements, or numbers of targets identified, or the identification of possible cyber or EW actions). To improve performance and confidence over time, testing and machine learning opportunities should be maximized over the life of the systems and updates to automated decision tools should be almost continuously issued at scale.

Countermeasures for Self-Protection: Countermeasures designed to defeat incoming attacks will have to earn their way onto the platforms in the concept based on their cost effectiveness. Current examples include active self-defense systems on armored vehicles.

Deception: The US has always under emphasized deception and the use of decoys or deceptive countermeasures.[16] Concealing the manned C2 vehicles should be very high priority. Part of this design challenge could be making them indistinguishable from other lower priority military vehicles or even from commercial vehicles. The UGVs are relatively high value targets in this concept; they carry multiple "archers" which carry multiple "arrows." Decoy UGSs could be very cheap and cost effective. They even open the possibility of anti-simulation, where some decoys can be less "decoy-like" and give the enhanced appearance of being the real targets— creating a

[16] One DARPA reviewer suggested making deception a warfare domain in itself. I wouldn't go this far, but it does need to be elevated in importance, in all domains.

false confidence that the "real" targets have been identified and engaged. UASs would rely on low level flight and concealment as well as favorable cost exchange ratios with some threats. Decoys could be used here to exhaust defensive munitions as a precursor tactic. The potential for operational level deception is also high with this concept and should be included in course of action planning and analysis.

Default Behaviors and Loss of Contact by Unit or Echelon: One operational contingency that would be of concern to the operational community is the implications of lack of contact or control over a platform or collection of platforms, which in this concept would include UGVs and UASs and ad hoc organizations composed of them. There would have to be programmed abilities to identify when this had happened and embedded tailorable rules at each echelon for how to best respond. There is no one optimal solution to this question; the "right" answer could range from "continue the mission" to "withdraw all units immediately" depending on the tactical situation. Setting these rules in advance is another human executive role that would likely be needed in the initial fielding of the concept. Because this can happen to any unmanned platform or group of platforms, it gets a little complicated, with different options for each possibility of concern or class of possibilities.

Energy: Current ground forces live on hydrocarbon-based fuel consumed in internal combustion engines. This includes fuel for vehicles and for generators for all supporting units. The potential exists for alternative forms of fuel for some applications, but I don't see any way to eliminate the need to refuel operational vehicles, both the UGVs and the UAVs in the concept as well as all the supporting vehicles. Even if, for example, fuel cells or all electric vehicles become cost effective and operationally viable, they will still need to be refueled periodically (in some form). The frequency of refueling may be much less. Current armored vehicles have to be refueled almost daily. A combination of much lighter weight platforms and more efficient technology should substantially reduce the operational energy burden, but the force will have to include the infrastructure to make some form of refueling possible. As noted elsewhere, that infrastructure including the fuel distribution and transfer systems will be highly automated.

Humans in The Concept: The location, role of, and support to humans is discussed under other areas and in the concept description. The bottom line is we must have some humans in the concept. Even though the numbers are reduced significantly, we still have to make provisions to support those humans, which will include command and control operators, special operators, and some logisticians. The survivability of these humans would be a high priority. It would be achieved primarily by concealment, deception, and keeping them away from engagements. Another notable feature of the concept is the military branch system (armor, infantry, etc.) may disappear, or be significantly changed. The branch system is based on the need for humans with highly specialized knowledge and training about some fraction of the force and certain equipment and units. In this concept the focus for humans is much more on integrated operations and the ability to supervise those operations and to interact with AI systems and automation–a more generalized and technical, but a highly specialized, skill set. In addition to designing the concept to support and sustain the humans in the system, C3BM systems (including AI based tools) will have to be designed to facilitate human interactions and to support human decision making where it is needed or required.

Infantry, or The Lack Thereof: The concept notably doesn't have infantry. That's because it is designed to fight a conventional force at scale and doesn't need them for that purpose. That opposing force would include mounted and/or dismounted infantry, but the concept is for the UASs, supported by the UGVs and long-range precision fires, to make massing and movement of both enemy vehicles and dismounted infantry untenable. Without vehicles, human infantry is slow, limited in carrying capacity, and needs extensive sustainment support. The concept assumes enemy infantry could be essentially fixed in place by the UASs and defeated over time, even if stationary concealment were temporarily successful. The infantry threat would be placed under continuous surveillance and covered by fires. It would be destroyed if it moved or exposed itself in an attempt to conduct engagements. As a result, neither infantry nor a robot-like unmanned platform with the mobility characteristics similar to humans is required in the concept for the driving force-on-force mission. For situations where human contact with civilians is inherent in the mission—peacekeeping, counterterrorism, and some counterinsurgency missions—armed humans will be part of the equation, but even in these environments it will be preferable to put unmanned systems rather than humans in harm's way whenever possible.

Interoperability: For the U.S. in particular, it is a strategic requirement to be able to work with allies and coalition members. In the past this has been given some attention in peacetime, but generally underemphasized, resulting in jury-rigged work-around approaches. The envisioned ground forces are likely to deploy into a situation where U.S. forces must operate in proximity to and in cooperation with allied units. Interactions at all levels, individual system, small unit, and operational levels are going to happen. In addition to combined operational planning and force management, provisions to ensure the safety of allied forces and to prevent engagement of U.S. forces by friendly allies will be required. Given the pace at which the concept I've described would conduct operations, and the supervisory role of humans, a lot could go wrong in a hurry. Cooperative designs and shared identification features that enable allied unit integration and to build confidence in unmanned system and collective behaviors is a necessity.

Legal Design Constraints: The lawyers are always with us. All our autonomous systems and the units mostly composed of them must follow the law, including the laws of armed conflict. There are also issues of liability for accidental damage to property and person, but these should be manageable under civil law approaches. Programmed behaviors and decision processes must take these constraints into account, but the operational concept won't work if legal constraints and decision-making has to involve humans in every situation. I've had the chance to observe, with admiration, how carefully legal concerns are weighed and evaluated in counterinsurgency and counterterrorism operations. We can tailor how this is done to the tactical situation, but in high intensity force-on-force ground operations there is no time for legal review of all tactical decisions. As a result, the automated rules of engagement must incorporate legal constraints effectively. For individual engagement decisions and small unit behaviors they must be part of the automated functionality. For mission tasking decisions they must also be part of the automated process, but where appropriate provisions should be included for human judgment and intervention. A good example is an assault or coordinated strike on a village where an enemy force is present but might be using human shields or where humans might simply be present. In another situation a similar

strike or attack against an enemy unit in an assembly area or moving to contact in low civilian density terrain would accommodate a much more automated approach. In even these situations, the combination of AI and human judgment may give a superior result. Consider all the devastating mistakes made in Afghanistan and Iraq with mistaken strikes on weddings and hospitals, even with the best of intentions. AI supported decisions should actually improve on this performance. The Geneva Conventions, including the legal obligations with regard to prisoners and wounded prisoners (see below) also have to be taken into account also.

Physical Security: For UGV systems, the designs must include some provision for vehicle and unit security from local threats. Modest hardening can provide a level of protection, but some self-defense capability is needed also. A nonlethal self-defense mechanism should be considered as a desirable part of the ground vehicles' suite of equipment, but one needs to be careful throughout the design about requirements creep. UASs could include anti-tamper and self-destruct features as desired.

Position, Navigation, and Timing (PNT): This service is essential to any domain including the land domain. GPS as currently planned is not secure enough to provide the required level of resilience. There are a number of technologies and combinations of technologies in various stages of fielding and development, but adequately resilient PNT must be part of the concept. Distributed autonomy, data fusion, and sound decision making of all types is totally dependent on PNT availability. This problem has to be solved for any future concept, highly autonomous or otherwise.

Prisoners of War: People have tried to surrender to drones in the past. In the concept I've described, that could well happen. Both UAVs and UGVs in the concept would have to be programmed to recognize an attempted surrender and respond correctly when that occurs. For UGVs at least, there would need to be an automated or semi-automated mechanism to accept a surrender and escort prisoners to a collection point, if circumstances permitted. Alternatively, prisoners could be kept in place under guard until processed. Wounded prisoners couldn't be treated but prisoners could be allowed to assist each other. Rules of engagement would also have to anticipate situations where prisoners tried to escape or reneged on their surrender. This is actually a complex issue, especially for dealing with an enemy who tries to surrender while under fire. We deal with it already, however. An attack helicopter pilot, for example, can't really accept a surrender. He or she has to decide whether to stop the engagement or continue. The unmanned machines in the concept will have to be programmed to do the same.[17]

Reliability: This was addressed earlier in the discussion of alternative models for sustainment. The platforms in the concept and their major subsystems must be designed with adequate reliability to function operationally long enough and well enough to be cost effective. High reliability, such as in long endurance space craft, can be very expensive, but that isn't required here. The absence of humans to maintain the systems forces a design for reliability trade-off that ensures adequate

[17] In the classic "Men Against Fire," SLA Marshall noted that experienced combat infantrymen in WW II knew that if they tried to surrender during a firefight that they would be shot. That environment doesn't permit split second decisions to stop shooting because someone puts their hands up and exposes themselves. The way to surrender with a chance of survival was to hide until the shooting stopped and then indicate your presence and intention.

confidence the concept will perform as needed at the aggregate operational level. It would be a mistake, as it has been for many military systems, to demand more reliability than is necessary or cost effective. It would also be a mistake to under specify reliability parameters. Anticipatory failure and fault monitoring to permit unmanned system self-evacuation prior to failure is also likely to be cost effective for some subsystems and components.

Responsive Threats: The first line of defense against the ground domain concept would be quick reaction counter-UAS systems and concealment. Based on DARPA experimentation to date, we can expect some novel attempts to defeat AI based detection and identification. The next would be attempts to design dedicated countermeasures exploiting weaknesses in the new threat. For the unmanned UAS and UGS systems in this concept, we could expect extensive EW and Cyber responses and dedicated counter-UAS weapons. Finally, we would see attempts to design and field forces that were similar to those described here, but superior in performance (longer range, more hardening, greater stand-off, more expendable, etc.) in areas deemed by the adversary to be operationally important.

Requirements Creep: Conscious attention should be placed on avoiding cost imposing marginal or low return on investment requirements. The natural tendency in all domains is to add more and more requirements to the design until the concept crashes from its own weight. A lot of the items on this list are good examples of potential requirements creep. The whole point of the concept is improved cost exchange ratios over current systems.[18]

Safety: This is always a design consideration. Some aspects of safety are covered in other sections, but unmanned autonomous systems will pose some unique problems and the very limited presence of humans in the concept may add some unique safety concerns. Without human operators, any number of risks that humans could have mitigated will have to be designed out or addressed through automation. The list of safety concerns includes electromagnetic radiation, chemical, electrical, mechanical, and explosive risks among others. It also includes all possible storage, transportation, or operating conditions the autonomous vehicles in the concept will ever encounter, in war and peace.

Single Points of Failure: A detailed design would have to carefully consider critical communications links and nodes and provide some combination of resiliency and redundancy where necessary. I don't see any obvious major problems in the concept from this perspective, but it has to be addressed. A thinking and capable opponent will certainly look for weaknesses in the concept to exploit. PNT, mentioned above is sure to be one area of interest. Others might include the ability to overwhelm the concept's tactical information processing capacity with an operational "denial of service" approach where the numbers of potential objects to be processed was overwhelming. Embedded cyber vulnerabilities are certainly on this list also.

Stealth: Some degree of stealth is important for the ground vehicles in the concept. While I assumed a conventional human intensive mechanized and/or infantry threat as the initial opponent, one has to assume that threat will include large numbers of UASs that can attack ground vehicles

[18] This item will occur in every domain.

(Azerbaijan and ISIS have demonstrated this.). It isn't practical to provide top and all-around hardening of ground combat vehicles against those threats, today or in the foreseeable future. The first line of defense, because of its cost effectiveness should be concealment through practical levels of stealth or camouflage. Signature management might be a better description. Part of the suite of passive defense measures could be movement patterns, use of terrain for concealment, and also signature management, in some cost-effective combination. UGS movement would be episodic and could be structured to be hard to correlate to traditional military unit movement. For UASs, signature management to some level should be explored as a design trade. Countering enemy surveillance systems to prevent targeting of all these vehicles, and especially the manned command and control vehicles would be a high priority.

Terrain Variations (forest, urban, built up, desert, mountain, swamp): The UGVs envisioned should be able to operate in all terrains with some limitations in each. Wheeled or even tracked vehicles with the payload capacity described in the concept have some fundamental design limitations. Because the UASs are the primary targeting and engagement asset and are not generally constrained by terrain, the biggest job of the UGVs is to get to where the UASs can be effective. This relaxes the requirements for those vehicles considerably. UASs in the concept could cover terrain inaccessible to the ground vehicles by observation and fires. To penetrate and secure structures the concept would have to include smaller unmanned systems that could operate in buildings. These could be transported by the UGVs and deployed directly from the UGVs or by the UASs. If the terrain cannot accommodate the UGVs, it cannot accommodate a mounted enemy force either. Dismounted enemy infantry threats will be discussed below.

Training, Experimentation, and Testing: The concept opens up some very cost-effective opportunities to design for training both the AI included in the concept, the humans that are part of the force, and the two together. The efficiencies come about because the human role is largely remote from the physical world in which engagements and tactical decisions are being made. This permits very realistic simulation and exercise construction in a virtual environment identical to the one that would be seen operationally. The human role is supervisory and much less physical than in current forces, largely eliminating the need for traditional field training. Training, experimentation, testing, and upgrades merge in this concept and would be all but continuous. Any operational experience should immediately inform both the humans, and the AI embedded throughout the concept.

Transportation: This was mentioned briefly in discussing the concept. There have to be assets that can get the combat and supporting systems and units to the battlefield. As today, everything in the land domain concept has to be designed to permit movement by a range of commercial and military means. In the future many of those transportation platforms will also be unmanned. As a result, the vehicles in the concept will probably have to be transportable in a combat ready configuration (fuel and ammo on board), or close to it. Movement of the force operationally could normally be organic, but some provision for at least intermediate operational airborne movement, by rotary wing or tiltrotor aircraft, would be needed to provide operational flexibility and agility, a form of vertical envelopment. These transportation systems would be unmanned transporters, and could serve a number of purposes: evacuation, resupply, operational movement.

Unattended Ground Sensors: There would be a potential role for these and at times the UASs could land and take on this role on a temporary basis. They, or the ground vehicles could also deliver sensors and emplace them. In some cases, unattended smart munitions could be included, with options for human control depending on the situation and in accordance with US policy (see the mine warfare discussion below). These systems could be recoverable or expendable.

Vehicle Recovery: UGVs and UGSs will self-recover as much as possible. If cost effective, at least some UGVs should have to the capacity to autonomously connect with and tow a similar size UGV to a recovery area. Highly damaged UGVs or those in complex recovery positions could be abandoned or recovered by special purpose vehicles. UASs may be recoverable by either UGSs or special purpose vehicles, but it isn't obvious what the cost-effective requirement would be. All vehicles should have some ability to auto-destruct or otherwise neutralize sensitive data and equipment.

Weather Implications: The concept must be designed to operate in a range of weather conditions, but not the most severe transient extremes. High winds and some visibility conditions could limit the UASs in the concept. The intent would be to adopt a more defensive posture during these periods. The insensitivity of unmanned systems to cold, heat, and humidity relative to humans would be an advantage.

Other Needed Military Functions

Air Defense: The biggest air threat to this force is small UAS systems operated by the enemy. These systems are already being fielded and used at scale, so this isn't a future hypothetical threat. Each ground platform would have some organic self-defense capability. This is likely to be a gun system which also would provide some self-defense against ground targets. A defensive suite may also include some soft kill capacity (jamming). Specialized unmanned ground platforms with directed energy systems are possible and would have to be distributed within the force. These platforms would be unmanned and would include soft-kill (EW and Cyber) capacity as well as kinetic kill. The small UAS systems in the concept could have autonomous counter-air capability as well, if necessary, with the possibility of dedicated counter-air munitions. Enemy launchers of UAS threats would be high priority ground targets. For both air and ground platforms, cooperative and non-cooperative identification- friend-or-foe (IFF) provisions might have to be included to preclude fratricide.

Civil Affairs and Psychological Warfare: These human intensive or human-centric functions are not the focus of this paper, but they would be considerations in any large-scale land operation, both those involving conventional forces and those associated with irregular warfare. The enemy's will to resist and support for, or at least acquiescence to, an occupying force are central to overall success of a campaign. The introduction of forces structured like the ones I describe, with high reliance on autonomous weapons, opens up some interesting psychological warfare opportunities. Any time human occupied areas are seized from an enemy there will be a responsibility to care for the population of those areas and restore civil government functions. It's beyond the scope of this paper, but collecting controlling, and managing information and the flow of information to the

enemy military and civilian population should be a key element of any operational campaign. Much of the work on commercial artificial intelligence today addresses the problem of persuading civilians to take certain actions—generally buying something. That technology should be directly applicable to these functions. In addition, the technologies associated with tracking the activities of entire populations through their interaction with the digital universe have significant utility here. It's a brave new world for civil affairs and psychological operations.

Combat Engineer Support: Some specialized units/platforms/mission modules for obstacle removal or creation, bridging, and demolition at least would be needed as would some construction capacity, but the going in intent would be to minimize the need for highly specialized vehicles and units. Specialized platforms like bulldozers, breaching systems, and bridging systems that might be used under fire would be unmanned and either autonomous or operated remotely. I don't see a high value or likelihood in the future of US forces needing or encountering highly fortified positions that would have to be assaulted. If they were encountered, the forces in them could in most if not all cases be fixed in place and isolated until they surrendered and/or were neutralized by fires.

Cyber and EW: Both are enduring threats and opportunities that require continuous attention in any concept, and in any domain. By putting as much decision-making capability into each autonomous platform as practical, the concept reduces the traffic that's required to the minimum. Cyber hardening has to be part of every design and continuously updated. EW hardening is necessary as well and has to be continuously updated. We need new paradigms and state-of-the-art capabilities in these areas no matter what. Offensive cyber and offensive EW are highly specialized and should be designed into the concept, probably in a mix of dedicated specialized platforms (manned and unmanned) and in some distributed capability, especially for EW as a secondary mission for all platforms. Software defined radio frequency systems open up areas for integration of communications, sensing, electronic warfare, and cyber to explore and incorporate in all future systems.

Disaster Relief / Humanitarian Assistance: I don't see this as a core mission for this concept. Some assets such as transportation assets could be useful and should be applied. Most current ground force humanitarian assistance is based on the large-scale human support capacity in the military. This concept is not human intensive, so capacity to provide medical, shelter, power generation, and subsistence support wouldn't be available in this force with the same density or volume as current forces. The ground force should certainly provide whatever it could, but that would be limited by the nature of the new concept and the much-reduced combat service and support structure it entails.

Intelligence Integration: The concept has to include automated tactical intelligence integration to support operational and tactical level planning including course of action analysis and the generation or update of the equivalent of an operations plan. Intelligence and operations are fully integrated in this concept and there is no significant lag between receipt of new intelligence data and planning updates. This elevates the pattern recognition problem to a higher level where the decisions being automated or supported are about unit planning at both the tactical small unit level

and higher as opposed to about selecting targets for engagement. This is where successful integration of data from multiple sources, including some in other domains (notably space and air in this case), becomes important and where humans still are likely to retain a role in command decisions.

Mine Warfare: Traditional mines are not very effective weapons; while individually cheap, they have poor aggregate exchange and cost per kill ratios. They also are expended in use and leave behind devastating long-term hazards to civilians. Their biggest role is slowing or channeling an enemy advance to increase enemy exposure to fires. Smart landmines can be more effective, but at a higher cost and under current policy with a heavy burden in human control. The US has appropriately all but eliminated traditional emplaced or scatterable mines because of the residual danger to non-combatants. The emotional effect mines have on humans advancing is of course lost when the advancing force is automated and unmanned. For the future force I have described, advancing against minefields can be accomplished in part through avoidance, particularly where the armed UAS systems are carrying the bulk of the fight, and if unavoidable through the sacrifice of some UGVs (purposely configured to be more expendable perhaps). Specialized mine breaching equipment is possible but may not be needed in the concept. I do not envision US forces needing to employ mines in the future concept.

Operational Planning and Rehearsal: at the platform and small unit level planning would be automated and rehearsals simulated, both with human monitoring and supervision, when practical. At higher levels, planning would still be highly automated, but with more human interaction and feedback. The cycle of immediate, mid-term, and longer-term planning—anchored by simulation—would probably still occur but be much more automated and integrated.

Rear Area Security: A fluid battlespace is envisioned for the concept, but there would still be areas of control for each belligerent, if not a well-defined front line. If there was concern about leave-behind enemy forces or partisans or a rear area raid of some kind, then some tactical forces could be allocated to rear area security. Some logistics systems and support areas would need self-defense capability, which could largely be provided by organic unmanned systems. I would envision tighter controls on any automated engagements in the rear area, up to and including human supervision of each automated engagement.

Special Operations: Ground special operations are currently particularly human intensive. Some of these missions, destructive raids for example, could be carried out by autonomous systems. Others might require humans for the foreseeable future—think the effort to capture Osama Bin Laden for example, or security assistance missions. I don't see the need for some traditional human special operations forces going away any time soon, but unmanned autonomous systems should certainly be integrated into those operations to improve performance and to reduce their risk.

Underground Combat (Tunnels): If this is considered a priority, specialized equipment may be needed. The smaller UGVs and UAVs envisioned for use in buildings should be of utility in tunnels as well. Tunnels are a problem that exists in the context of permanent border situations or in attacking forces that have had a long time to prepare defenses in situations like urban areas. I didn't consider this a major driver for the land domain concept, but it can't be ignored entirely.

Warfare Domains – Sea Surface

Introduction

It's been an interesting exercise to watch the Navy struggle with what to do with unmanned surface ships. Assistant Secretary of the Navy Sean Stackley and I were discussing this topic several years ago, and he asked me, I think appropriately, "What mission would they (unmanned ships) perform?" It wasn't a rhetorical question--neither of us thought at the time that the Navy was anywhere near turning an existing mission over to unmanned vessels, (with the exception of mine hunting and clearing) and until someone answered that question there wasn't a lot of point in buying several unmanned ships, which was being advocated at the time. The Navy, I'm afraid, still hasn't answered the question, although it is continuing with the acquisition of modest numbers of experimental unmanned surface ships of various sizes. The Navy has also created an organization dedicated to unmanned surface vessel experimentation and released an overall unmanned "framework" document.[19] The problem in part, I think, is the Navy is looking at unmanned ships as augmenting and complementing manned ships of the types currently in the fleet. There's another way to approach this.

Operational Concept

As we did for land systems, let's start with a clean sheet of paper and expand our thinking. The reason we have manned surface warships is to provide sea control, protect shipping lanes or at least the ships in them, and project power. This includes the ability to protect international freedom of the seas and commerce, defeat other countries maritime assets—surface and subsurface, attack enemy land targets in support of air and land campaigns, support our allies, to protect the movement of land forces and freight to overseas theaters, and to support amphibious operations. Naval vessels also perform a "show the flag" mission to communicate to others the facts of US presence and power, and to support diplomatic efforts. We ought to think about three questions, each of which would provoke a strong reaction from any Naval Officer.

First, do we really need surface ships at all to perform these tasks? With foreseeable systems and technology, it is probably more efficient to perform a large fraction of the sea control mission from places other than the surface of the sea. For surveillance and targeting purposes, airplanes and satellites have much shorter movement times to an area of interest or, in the case of on-station geosynchronous satellites, none at all. Those systems can see much wider areas than surface ships. If sea-based surveillance is considered necessary, a large deployment of unmanned monitoring stations would be trivial in cost compared to manned warships. The seas are already being monitored from a range of satellites and sea buoys as well as from commercial shipping. Some years ago, I had one of my staff do a back of the envelope calculation on how many unmanned

[19] My experience with strategy documents of this type coming out of the Pentagon's consensus-oriented bureaucracy is that they are aspirational as opposed to firm, and rarely provide meaningful plans or commitments.

wind mobile and solar powered floating sensors would be needed to continuously monitor the surface of the Western Pacific; he calculated that the whole job could be done with 1,000 small autonomous platforms at $1 million apiece or for about $1 billion, much less than the cost of a single warship.[20] These assets could be attacked of course, but that would be a hostile act and the lost assets would be relatively inexpensive to replace. If delivery of weapons is the goal, there may be more efficient platforms than surface warships. Warships are largely launcher, sensor, and projectile magazine transporters. Shore-based bombers and land-based conventional cruise or hypersonic missiles can achieve much faster time on target, unless the warship is already in fairly close proximity to the targets of interest. While surface ships can have fairly large magazines, air assets can also be reloaded and complete multiple sorties in a fraction of the time it takes a manned warship to return to port, be rearmed, and move back on station.[21] Aircraft carriers and surface ships can stay on station for long periods, but carriers must be replenished with aviation fuel and munitions frequently, and those auxiliary logistics assets are vulnerable to attack. Bottom line, it may be much more efficient to control the surface of the sea from space, the air, and land then from surface ships—if adequate situation awareness can be provided by some other means.

Second, if ships are cost effective for some tasks, do we need people on those ships to perform the tasks? If one thinks of the ship as a black box that delivers certain capabilities—air defense, surface and subsurface attack, and land attack—there isn't an obvious reason why those black boxes have to contain people. A surface ship is a combination launcher and transporter with a suite of sensors, self-protection devices, and C3 capabilities. The people are on it to control those functions and take care of the ship. If we can reliably automate or remotely control those functions and the ship doesn't need people to take care of it, there's no compelling reason to have people on board.[22] The US Navy years ago moved toward substantially reduced manning on newer design ships. This is enabled by increased automation, system integration, and high reliability. Unmanned autonomous surface ships have been built to various scales and performed successfully on extended voyages. More are under construction. Small solar and wave and/or sail powered unmanned vessels have also been built and used fairly extensively. Commercial shipping is minimally manned today and experimenting with unmanned concepts.

Finally, there is the serious question of surface ship survivability, independent of whether a ship is manned or not. One of the most significant unknowns in modern warfare is the survivability of warships against state-of-the-art threats—especially anti-ship missiles. Modern warships have fairly capable defenses, but once a capital ship is targeted today it is likely to be attacked with large raids of sophisticated anti-ship missiles designed to work together to penetrate the individual ship's defenses and any formation of ships' integrated defenses. Layered defenses, remote launch

[20] The concept was based on larger scale versions of products currently produced by a non-traditional defense contractor called Saildrone which was funded in the early days of the Defense Innovation Unit Experimental (DIUX).

[21] Current US Navy ships cannot have their vertical launch cells reloaded at sea. Attempts to remedy this shortfall have been unsuccessful.

[22] A traditional reason for large crews, coming out of the WW II experience, is the need for people for damage control, especially firefighting, if a ship is hit by enemy fire.

cooperative defense, and a range of soft-kill mechanisms and deception can all be deployed against the attack, but as a former Air Defense officer and a systems engineer who worked for years on tactical and strategic air defenses, my money is on the attacker. The numbers game favors an attacker; even theoretical layered, statistically-independent, high single-shot probability of kill defense systems can be overwhelmed. Only the attacker knows for certain what creative tactics, techniques, technology, and attack strategy he will employ. Probabilities of successful engagement have to compound over many attackers, and defensive missiles can be simply exhausted. A major problem today is that no one knows with any accuracy just how effective shipboard defenses would be against a modern threat. There have been some limited engagements, but there has never been a many-on-many engagement of current state of the art anti-ship missiles in a coordinated attack on a modern warship or formation of ships. We may well find out the hard way someday how effective our defenses are—or are not. We can test and simulate of course, and we do, but the Navy has in my experience resisted extensive high fidelity testing and the simulations, and models in use are only as good as the data that goes into them. Resolving the question of surface ship survivability in a highly contested environment has to be central to future warship design and operational concepts, but that's not where we should start. We should start with the question of what missions need to be performed in the sea surface domain and what is the best way to perform them.

Those at all familiar with the way the Navy thinks about the Navy's missions in warfare have probably recognized by now that I'm not talking about the Navy's standard terminology of Anti-submarine warfare (ASW), Anti-Surface warfare (ASuW), and Air Warfare (AW). I think those concepts bring with them a certain way of approaching surface ship missions in terms of the targets one wants them to destroy as opposed to the missions one wants them to perform. There is a lot of overlap, but I'm trying to avoid starting with the assumption we are talking about manned or unmanned surface combatants that need to kill certain types of targets and then optimizing the list of mission capabilities we want to get into a surface combatant hull to perform some mix of those tasks. If ships are expensive, vulnerable, and limited in speed, endurance, horizon, and mobility, then it may make sense to let platforms that don't have these characteristics do many of the jobs traditionally done by surface combatants. We only need to design operational concepts and corresponding ships for the situations where surface warships are the preferred tool. My provocative conclusion: this may be a fairly limited set of missions, given what can potentially be accomplished more cost effectively from the air, space, land, and undersea environments.

Let's start with the traditional navy mission of destroying an adversary's surface navy. Naval warfare history is largely about fleet versus fleet engagements—Trafalgar, Jutland, Midway, and Leyte Gulf for example. The history is that until recently there was no way to destroy an adversary's navy at sea except by creating a better navy, with some mix of superior quantity and quality. Other factors have mattered too: leadership, tactical brilliance, and training to name a few. Nevertheless, technology has always driven the evolution of naval warfare in fairly clear ways. Vessels propelled by oars that rammed opponents gave way to short-range cannon; wood and sail gave way to steel and steam; battleships with heavy guns and line of sight gunnery gave way to aircraft carriers with short-range aircraft carrying gravity bombs and torpedoes; and most recently

carrier-based aircraft with stand-off anti-ship missiles and ship-launched long-range anti-ship missiles. The constant in this evolution has been increasing engagement ranges away from the ship that carried the weapons, or in the case of the carriers and our construct, ships (transporters) that carried the launchers (tactical aircraft) that carried the projectiles or weapons (missiles). The reason ships were necessary to this construct is that until relatively recently, land-based systems lacked the range to deal with a distant enemy naval force. WW II in the Pacific was largely about acquiring islands from which fighters could provide air superiority and support to ground forces and from which land-based bombers could strike deeper and deeper into enemy territory. Because enemy fleets guarded those islands and posed a threat to our sea-based amphibious and naval forces; naval assets—carriers primarily—had to be employed to attack the enemy's fleets and to suppress land-based aviation until it could be neutralized or overrun. When one compares the ranges of both aircraft and missiles today (1,000s of miles) to the ranges available then (100s of miles) and when one throws in the continuous surveillance now available from space—it's a different world. Maybe it's time to rethink some fundamental assumptions about how the surface of the sea is controlled.

Aircraft carriers are expensive transporters of launchers and projectiles. They are extremely high priority targets for our adversaries and during operations have to be continuously supported by refueling and rearming support vessels, which are also subject to attack. They are inherently limited in runway length and the size of the aircraft they carry—effectively limiting the range of the aircraft they can carry and making them increasingly difficult to hide from a sophisticated enemy, especially when they are conducting flight operations, which restricts maneuver options because of the need to create wind over the deck.[23] Because of their small numbers and high operational value, other resources have to be devoted to protecting them from a range of threats, including air, surface, and subsurface threats. At one time, through the end of the Cold War, a reasonable case could be made for the survivability of carriers. When I was Deputy Director of Defense Research and Engineering for Tactical Warfare Programs at the end of the Cold War, the Navy had convinced me it could conceal what was then called a Carrier Battle Group from detection, at least for an operationally useful period of time. This is increasingly difficult to assert convincingly. As threats have grown, the Navy has acknowledged that carriers cannot operate within operational range (a few hundred miles) of a sophisticated adversaries' shorelines. As shore-based aircraft and weapons ranges extend, there comes a logical point when there is nowhere left for carriers and surface combatants to operate. At one time carriers were the dominant surface control platform because of their aircrafts' lethal reach compared to guns. With long-range anti-ship missiles widely available, that is no longer the case. In modern times, carriers have been used to provide continuing and cost-effective counter-air and strike operations over land, but not against peer competitors. Against lesser threats, this will be an enduring virtue and a good reason to keep the carriers now in existence, but it is not a strong argument to continue purchasing them at current rates indefinitely or to maintain them as the centerpiece of a sea control force.[24]

[23] To launch fully combat loaded aircraft, carriers generally have to steam into the wind to create wind velocity over the deck, effectively adding about 30 knots in relative velocity to the take-off speed of launching aircraft.
[24] One can also make a case that carriers are useful after a sophisticated enemy ability to conduct long-range engagements against carriers has been destroyed or suppressed by other means.

So how should a future force be structured to defeat other countries' navies, support or enable power projection, assure the safe passage of commercial shipping, and to provide sea control, especially far from the territorial U.S.? Let's start with the mission to defeat an adversary's sea-based power projection fleet. For the U.S., a goal here is to apply enough lethal counter-ship fire to defeat an invasion fleet operating against an ally or friend, such as Taiwan. As China increases its naval capacity to threaten Taiwan and assert its regional maritime claims this becomes a pressing question. (This is almost the mirror image of the problem China has defeating U.S. power projection from the sea, except China has a land mass to operate from. China has chosen to solve this problem largely with land-based mobile anti-ship missiles along with other assets.) The first requirement is the ability to continuously detect, track, and monitor the adversary country's naval assets with targeting quality information. Ships are large and they have multiple signatures—visible, thermal, radar, and acoustic. They also produce wakes and must emit signals to perform some military functions. An autonomous distributed network of surface-based sensors in an USV surveillance architecture concept was discussed earlier, as was space-based monitoring. Space would seem to be the most cost-effective approach to achieving this goal, if survivability or at least resilience could be assured (more about space survivability later). Unmanned long endurance aircraft, possibly cued by other assets are another possibility. In a robust force, some combination of space, airborne and sea surface systems (all unmanned and autonomous) would be the most resilient approach, and should be affordable. There are trade-offs among these options, but there is a high premium for redundancy and resilience. Let's assume for now this problem is solved with a mix of reconstitutable, continuous, and long endurance surveillance systems with secure communications to resilient and survivable command and control centers from which engagements can be planned and directed. Our next goal is to provide the most cost-effective way to conduct those engagements. The target set for a peer competitor like China is nominally at most a few hundred vessels. If we are trying to halt a sea-based invasion of Taiwan, we would have a requirement to attack those targets within a few hours. We might have some period of strategic warning, a few days say, in which to mobilize and move assets closer to the target set, but let's assume we don't have that luxury to the extent we could move surface ships or submarines on station, which would require several days at least. We can expect the naval forces of concern to be reasonably well defended, with some long-range counter-air capability extending out to a few hundred miles and reasonably robust terminal defenses. Our projectile of choice is going to be anti-ship missiles, cruise certainly and possibly ballistic and possibly hypersonic. One could consider torpedoes or sea mines as well, and I wouldn't rule them out entirely, but a number of considerations suggest that missiles make more sense against time-sensitive massed targets like an invasion fleet. (I'll cover submarine launched torpedoes in the subsurface domain section.) Air delivered torpedoes with ranges of over 20 miles nominally could circumvent terminal air defenses, but limitations of range, deconfliction problems with multiple targets, time on target, and delivery problems argue against them. This brings us to a trade space for projectile or missile type and range, and for potential launcher range, capacity, and type. If land is available for the launch platform, that seems to be a preferred option, assuming mobile launchers, especially as with Taiwan where we know the likely invasion target already. Land basing for anti-ship cruise, ballistic, and even hypersonic missiles provides opportunities for mobility, concealment,

hardening and deception, all of which are valuable against a sophisticated opponent. Land basing is favored if there is relatively local basing, probably out to something up to 1,000 miles from anticipated engagement areas so missile range and therefore cost can be less. Shorter range reduces cost, but it also reduces flexibility, so the "right" answer isn't obvious. If suitable land isn't available air-launched systems would seem to be the next best option. Airborne launch platforms can be on station fairly quickly, are flexible in where they are applied, and with adequate standoff, the delivery platforms (launchers) should be survivable. They also offer some modest extended range by virtue of launch at altitude vice surface launch. For a country like the United States, the best trade-off between weapons range and launcher range would seem to be to acquire enough weapons range to provide for survivability of the launching aircraft through stand-off, and no more. The launching aircraft is reusable, and the weapons are expendables, so lowering the cost of the weapon while tolerating some increased cost in the launcher makes sense. This gets more complicated when aircraft base survivability is factored in, which it definitely should be. (More on that in the air domain section.) The range and other features such as capacity and cruise speed of the airborne launcher is also dictated by the geography available to the acquiring nation and the amount of time needed to conduct engagements in the threat scenarios of interest. All of this needs to be investigated through trade studies, but the first question we should try to answer objectively is whether or not it is now more cost effective to use non-sea-surface systems to defeat an opponent's surface naval forces? I believe the answer is likely to be yes, and this has major implications.

Succinctly put, it leaves us with the problem of figuring out what missions one needs surface combatants for. If carriers aren't the preferred way of projecting power ashore against a peer competitor, and surface ships in general (carriers and large surface combatants) are not the preferred way of attacking an adversary's fleet of surface warships, what's left? What are the tasks or missions for which surface combatants (manned or unmanned) provide cost effective military capability?

I think we have at least three missions to consider where surface ships have a potentially attractive role. We still want to provide cost effective defenses for non-military shipping, which prioritizes being in continuing proximity to the ships we want to protect as they move. We still want to provide continuous control of key maritime terrain where we might not have land access—choke points for example. We may want to provide on station quick reaction and responsive high-density strike or fires capability from the sea—in support of an amphibious assault or raids for example. Even if we rely on airborne and space-based assets for surveillance and targeting, there is also some merit in having a redundant sea-based sensing and continuous surveillance capability. What these missions have in common is the need for continuous presence and responsive fires. Surface ships on station or accompanying protected assets offer that important feature.

The first task future surface warships could perform relatively efficiently is the protection of other ships, or escort duty. The U.S. is in the position of being separated from the places where we would expect to be in conflict with a great power by large oceans. We are also dependent on global trade, primarily by sea. Our allies are on the other side of those oceans for the most part. Moving anything of substantial aggregate mass, like a large conventional force and all its support equipment and

logistics, a long distance across oceans is much more efficiently done by sea. Transport by air is reasonably efficient for thousands of people, but not practical for deploying the many tens of thousands of tons of equipment associated with large scale conventional forces and the logistics support for those forces. This is likely to still be true even for the largely unmanned ground forces described above. The surface vessels that do this task are subject to attack on short notice and can best be defended by escort vessels that move with them and are designed to defend themselves, and the vessels they accompany, against air, surface, and subsurface threats. Commercial shipping is moving toward unmanned vessels as well, and one can imagine a convoy of sorts consisting of unmanned cargo and escort vessels. Because the overhead associated with placing a small crew for command and control purposes on a commercial size ship or escort vessel with a reasonable sensor suite and munitions magazines is relatively small—a few percent of the capacity and mass of the vessel—the delta cost associated with keeping some humans aboard may be small enough to justify doing so, if only for unforeseen contingency purposes and to have someone "in possession" of the vessels.[25] One could envision some manning in peacetime and low risk situations, but removing the humans for high risk missions. Escort vessels will be expensive enough under any circumstances that high attrition would not be very acceptable. They would provide the last layer in a layered system of defenses—the terminal defense co-located with the defended assets in the traditional layered defense construct. Outer layers would be provided by other assets, to be discussed shortly, that would be responsible for broader sea and air control.

For the land warfare section, we assumed a force-on-force construct between a conventional current design force and a highly automated force. Here let's start by assuming our problem is getting commercial shipping from the US to an ally in Asia successfully against an array of conventional threats: sea surface, undersea, and airborne. I don't expect China to restrict its military forces to within the second island chain. The concept is a tactical grouping of optionally unmanned autonomous vessels configured for the mission with a mix of weapons and sensors in a modular payload design that is loaded out consistent with threat expectations at the start of the mission. This tactical grouping can conduct ASW and ASuW missions, but it is primarily sized for dealing with missile attacks whatever their origin. It would have to provide some degree of layered defenses, support extended range launch on remote engagements, launch on warning, and terminal defense. The team of vessels would integrate on-board and off-board sensor data in a coordinated air picture and engagement strategy. Against large raids all engagements would be automated.

The weapons (projectiles) on the ships (transporter/launchers) are primarily going to be missiles. There will be substantial numbers of them and various types. There would be a standardized launcher system on the ships with various load out options. Missile range and payloads and mix are tradeable and can be tactically adjusted, but the escort group would have to fight with whatever is loaded at the start of the mission/voyage. The ships involved have to carry reasonable payloads, but not have too many eggs in a single basket, and they have to be vessels that can move with and

[25] One DARPA reviewer disagreed. His point was that zero-manning opened up previously unthinkable design ideas. One example he provided was removing threatening boarders by completely rolling the ship, something not likely to be considered in a manned ship design.

somewhat more dynamically than the ships they are protecting. Sensors for the anti-missile mission can be a combination of off-board and on-board and passive and active. At least some of these escort vessels might include rotary or possibly tiltrotor ASW/surface surveillance UASs. When all this is put together in a package it looks roughly like something in a frigate or destroyer size class of ship.

As indicated, the escort vessels provide the close-in defense of the protected shipping. Outer layers are provided by airborne assets that can target sea surface threats and as much as possible by land-based systems, when possible, as well. The hardly original idea here is to destroy the archer not the arrow as much as possible. We discussed wider area sea surveillance and land-based and airborne engagement systems earlier. If some threats—surface, subsurface, or airborne "launcher" platforms—through a combination of deception, stealth, and good luck get within missile or torpedo range of the protected fleet, then the escort force also provides the final protection against those threats and their weapons.

An idea worth considering to augment this capability would be placing transportable mission modules on the commercial ships being escorted.[26] Both weapons and sensors could be carried and integrated into the defensive architecture. One could consider even substituting this capability for the dedicated military surface vessels described. My view is that some multi-role military capability is needed and can only be provided by dedicated vessels.

Our next surface combatant mission of interest is to provide continuous control of key maritime terrain where we might not have proximate land access—choke points for example. In this situation we are trying to prevent an adversary from transiting an operationally significant waterway. We may also be trying to protect the transit of friendly shipping. Here we are concerned with preventing a moving adversary force from transiting a fixed area at a time of his choice or with protecting friendly assets as they transit a fixed location where local threats exist. (For engineers, a Eulerian vice a Lagrangian frame of reference.) This is different in fundamental ways from protecting a moving set of friendly assets in the open ocean. Think Straits of Hormuz or Malacca for example where no local power will allow the U.S. to conduct operations from land, or an exit route from an Arctic bastion. In this situation we have a need for continuously on-station, sea-based engagement capabilities of various types with relatively short times of flight to the area of interest. The number of places where this situation would arise for the U.S. may be relatively small. In most of the world we have allies who might be willing to have U.S. counter-sea systems deployed on their land, as long as those assets were used to defend the ally in question. It might be highly problematic to use those assets otherwise, however, so sea-based capabilities would be of value.

What we are trying to do here is to bring timely fires on a set of transiting surface targets. The fires again are primarily anti-ship missiles. The launchers for those fires can be surface ships with weapons range stand-off from the sea area of interest. That range would nominally be a few

[26] There's an analogy to the naval gun crews and weapons placed on merchant marine shipping in WW II. My father served on one of these details in the Atlantic late in the war, after having served for most of the war on a destroyer in Arleigh Burke's Little Beaver Squadron in the South Pacific.

hundred miles at most so that time of flight was reasonable for tactical responsiveness. The concept is essentially an arsenal ship. Fires could be cued and receive target tracking and updates from space-based or airborne sensors. Synchronized raids could be planned and released using on-board or off-board command and control capability. US surface ship survivability would be through stealth if possible. At one end of the spectrum this concept is basically a barge with munitions. At the other end it is a well defended magazine with a mix of defensive and offensive weapons. The escort vessels discussed earlier, with a different projectile load out could perform this mission. However, as I think about this operational mission, I'm not fully persuaded of the need for this capability from naval surface ships. Other concepts, such as on-station unmanned submersible weapons carriers might offer advantages in cost and survivability, but with some disadvantages as well. If global surveillance is maintained through successful space control and or cuing is available from whatever source with the lead time needed to put aircraft weapons carriers on station, the need for and advantages of surface combatants are lessened.

Finally, we may want to provide on-station quick reaction high density strike capability from the sea. This could be a requirement in an amphibious assault or a raid for example, or in support of allied forces engaged on land. This situation implies a requirement for large amounts of relatively close on-station fires, over the horizon but within say 20 to 100 nautical miles. Fires would need to be both preplanned and responsive as needed. The timing of those fires, within some operational window, is primarily our choice, although external factors such as weather and enemy movement or synchronization with friendly forces could easily affect the specifics. In addition to fires or strike, this mission would also bring a requirement for local air defense against anti-ship missiles. The construct described for commercial shipping escort mission would also seem to apply here, but with the addition of modest range offensive fires. One can also envision arsenal ships with a mix of fires and sensor platforms and C2 platforms in some combination. The building blocks could be common with the escort vessels, and those in the choke point discussion (commonality improving the argument for that capability), but again with a different weapons load out or mix of load outs in each case.

Building Blocks

For control of the sea surface domain, we are left with a combination of a global C3BM system that integrates space, airborne, and sea surface unmanned sensors; long-range shore-based strike aircraft with medium range anti-ship missiles, land based anti-ship missiles, and surface combatants. I'll discuss the surface combatants here.

The basic surface combatant building block is a vessel with a suite of sensors and with the capacity and flexibility to carry a variety of weapons for either defense or strike missions. The vessel displacement would be in the nominal range of a mid-sized surface combatant—several thousand tons. The vessel could be "optionally manned" given that the overhead associated with a small crew for command and control would be modest. For a given multi-ship mission most vessels involved would not have to be manned. We should be reluctant to rely on remote off-board C2 when operating against a sophisticated opponent with the capacity to mount a mix of EW, Cyber

and kinetic attacks on communications systems and nodes, but we should be able to achieve secure local command and control of an operational formation of several vessels. Stealth is highly desirable which implies low passive signatures in all wavelengths, a preference for passive sensors, and low probability of detection active sensors. Getting the balance of features "right" in this class of vessels will be a major challenge. Those features include stealth, protection against the range of threats, the sensor suite, countermeasures of various types, hardening, hosting of assets such as UAVs, damage control features, reliability, sustainment costs, and on and on. This mix isn't much different from current design trades for a multi-role surface combatant like FFG(X), but the emphasis on survivability would be much higher than in current designs and there would be design challenges associated with autonomous unmanned operation. Networked and potentially autonomous operational capabilities at the level of a multi-ship formation would be important for a number of functions—strike planning, air defense, and maneuvering for example.

In this concept the unmanned surface ship serves as transporter and launcher. The projectiles are predominantly the missile systems for strike or defense carried by the USV. These would be evolutionary extensions of current missile systems.

Complexities

Cross Domain Considerations: Surface forces can deliver cost effective multi-domain effects, but they also have some critical multi-domain dependencies. Surface forces can provide support and effects to Anti-submarine Warfare and Anti-air warfare, space surveillance and engagement, missile defense of ground targets, and naval shore bombardment or strike. I'll discuss each of these missions below. However, because of the limited horizon of their organic sensors and the need to stand-off from anti-ship threats, surface forces will be highly dependent on space assets and airborne assets for situation awareness and targeting for effective long-range engagements, in all domains. Surface forces will need to operate far from higher echelon command and control and will be dependent on reliable long-haul communications. Surface forces are also likely to be part of a multi-domain force that conducts integrated space, air, surface, subsurface operations and support to operations ashore as an integrated whole. The concept provides for the option to have some humans for command supervision on some or all of the surface warships, but even with that feature, the need for reliable multi-domain enabled communications to support operations is an absolute requirement in every mission.

Logistics: Warships have to stay at sea and operate for days, weeks, and even months without a return to port for maintenance and resupply. Nuclear propulsion aside, Navy vessels on station for long periods or conducting operations need to be refueled and resupplied at sea. It would be beneficial if munitions could be resupplied at sea, but today they are generally not, with the exception of weapons delivered by aircraft from aircraft carriers. If we take the humans off the ships, some consumables and services are no longer necessary, but automated refueling and if possible, rearming would still be required for the foreseeable future. In addition to resupply, maintenance needs for the many complex systems on a warship have been a major driver of crew size and composition. For the concept I've described to work, the design must be highly reliable,

for the vessels themselves and for the systems they carry. I don't believe these requirements are unachievable or unaffordable; we are seeing similar requirements being met by other systems, but high reliability and at sea automated logistics support will be necessary unless we limit the envisioned warships to short duration missions. It isn't hard to imagine automated refueling. The Navy has attempted concepts for at sea resupply of munitions like Standard Missiles and Harpoon but has never been able to implement a system. This is worth another attempt, particularly in the context of new designs that are not wedded to current standard Vertical Launch System (VLS) configurations.

Target Identification/Collateral Damage Avoidance: The sea surface uses of anti-air, anti-ship, ASW, and land attack are all going to have stringent requirements for accurate target identification and avoidance of false positive and false negative errors. For the most part surface ships will rely on target identification provided by off-board sensors. In many cases surface ships will be receiving engagement orders and the actual engagement decision will be made at a higher echelon battle command node. In some cases, data may be merged or fused on a ship to make a target classification decision on the warship, but I expect this to be the exception. For defense against large missile raids, the rules of engagement may be preset at a higher echelon, with individual ship and even flotilla level decisions made locally. On board sensing dependency will occur in some self-defense situations against air and small boat threats, especially in times of tension short of hostilities. In those cases, the actual decision may be made autonomously on the warship, but it is more likely to be made with human supervision or direct control of any engagements—either remotely or locally.

Design Requirements and Considerations

Anti-Tamper: The potential for a sophisticated opponent to acquire physical access to a warship has to be considered. Ships are lost at sea for a variety of reasons, in peace and in war. While we would try to deny an adversary access to any vessel that had foundered or over which we had lost control, this can't be guaranteed. Critical functions will have to be designed with state-of-the-art anti-tamper. In addition to protection from physical and cyber hands-on reverse engineering, remote cyber-attacks must be hardened against with high confidence. An obvious potential vulnerability for autonomous warships is that control could be lost to a hostile actor. To some extent this risk exists today for manned vessels also. Provisions for physically destructive anti-tamper and/or scuttling (either autonomously or on command) have their own risks but could also be included in the design.

Arctic and Antarctic Operations: I don't foresee significant design requirements coming from the need to operate in these environments. The Arctic especially will be contested and there will be increased commercial traffic and activity. As a result, the U.S. will need to protect assets in this area and attack adversary assets there, so warships will have to be designed to operate in arctic environments. Some design requirements will flow from the unique environmental features and

threat possibilities in these areas. Ice breaker capability may be required and could be provided by manned or unmanned vessels.[27]

Auxiliaries: The Navy ship inventory currently includes a large number of specialized auxiliary vessels for various purposes including replenishment and refueling, intelligence collection, ocean research, tugs, tenders, rescue and salvage, and command and control ships. The suite of auxiliaries needed to support the envisioned concept, in peacetime and in conflict, would have to be reconsidered completely. The survivability of these ships is low against future threats, so more resiliency would have to be designed in for future auxiliaries to be compatible with the operations of the new warships.

Civilian Engagement and Interaction: One attribute of current manned platforms is their ability to "show the flag" through foreign presence and port calls. Combatant Command leadership values this capability, as do diplomats. There are also a number of actions manned vessels can take, such as assisting vessels in distress, counter-narcotics and counter piracy operations, and blockade or sanction enforcement, for example, that bring naval vessels in contact with civilians at sea or on land. I don't see these human-centric missions being automated any time soon. For that reason, I think there will be a need for some manned naval vessels in the force that can conduct these types of operations. I'd place them in the rough design category of the Coast Guard's Heritage Class Offshore Patrol Vessel.

Collision Avoidance: This is a basic requirement. All marine vessels are required to follow international and national collision avoidance rules called "COLREGS." At this time there has been enough experience with unmanned supervised and autonomous vessels that I don't foresee this as being a major design obstacle—if not already, then in the near future.

Confidence In Automated Behaviors: For surface ships and surface ship formations, the confidence in automated behaviors has to be extremely high and high across a lot of critical functions. Ships are big, and putting one in the wrong place at the wrong time has major consequences, as we have seen in recent U.S. Navy history. (Although arguably a well-designed autonomous system might have done better than the crews involved in the recent collisions at sea.) At this point in time, driven by economics, commercial technology seems to support unmanned ground vehicle navigation, at least on developed road systems. Taking the cost of a driver out of a taxi or a truck is a more significant impact than taking the cost of a helmsperson off a capital ship. Nevertheless, there has been a lot of international development in autonomous vessels. It isn't that the ground vehicle problem is easier; in some ways it's harder; the ground environment is more non-uniform. However, the steps a ground vehicle has to take to avoid a serious accident are simpler and faster than those for a surface ship, and the consequences of errors are not on the same scale. One notable feature of capital ships, unlike ground vehicles, is that they have a hard time stopping and turn relatively slowly. For automated behaviors associated with tactical decisions about engagements, the potential to engage a commercial airliner or a non-combatant vessel also carries heavy consequences. I would argue, however, that in a peacetime period of tension the absence of fear

[27] There has been long running, and until recently unsuccessful, attempts to get the U.S. Navy or Coast Guard to fund a small number of icebreakers.

by those aboard for their own safety and the safety of the crew might substantially reduce the risk of an unwarranted engagement. The decision standards for wartime scenarios would be substantially different and tailored to the specific operational and tactical situation. In any event, I believe we can attain and verify acceptable levels of confidence in these decisions, especially in a hostile environment where most threats are distinctive and provide clear signatures. Tactical reality in the form of the time window to order defensive engagements against large attacks forces us to automated decisions in any event.

Construction (Seabees): There will still be some needs for forward and expeditionary shore installation construction to support the fleet. The degree to which this is needed, and the specific capabilities would be dependent on the theater and types of operations planned. This support function would largely utilize state-of-the-art commercial construction technology

Countermeasures: Countermeasures designed to defeat incoming attacks will have to earn their way onto the platforms in the concept based on their cost effectiveness. Decoys like NULKA and EW systems like the SLQ-32 are good examples. These can be very high-payoff investments, but they also carry some degree of risk associated with unknown threat responses. Automated processes and streamlined, even real time, software upgrades should be the norm in the future.

Cyber and EW: Electronic Warfare capabilities of various types would be integrated into the warships in the concept. The radio frequency design features of the system would need to be integrated to balance and optimize several goals. I can envision a radio silent mode which combined with other signature reduction would make targeting problematic for the adversary. Once concealment has been broken, the need for effective RF support to close in surveillance and engagement takes priority and active countermeasures would be enabled. AI technologies for "smart radars" communications systems and EW integration and machine learning are being developed now and would be included, along with the capacity for near continuous, if not real time, updates. Cybersecurity would be a necessity. Active use of cyber to defeat attacking systems or against threat defenses is also a possibility that should be pursued and included in the concept.

Damage Control and Resiliency: One of the main reasons to have crews on warships has been their utility in damage control. Over time the Navy has moved to more automated systems, but not entirely. The very flexible and adaptive ability of human beings in a complex damage-induced crisis won't be replaced by automated capabilities anytime soon. The design in this area will have to accept that fact and do as well as is reasonably cost effective to install damage limitation and reaction systems. Requirements for the resiliency of onboard weapons systems and the hull, mechanical, and electrical (HME) design to attack provide a broad trade space all the way from "ignore it" to design for continued operation despite multiple hits. The right balance is somewhere in between of course, but the trade space looks very different when there are no people or a few people in a limited role to be protected, as well as the vessel itself to consider. Absorbing at least one hit from most classes of weapons and not sinking seems like an entry level goal. Next on the hierarchy would be retain the ability to maneuver and self-evacuate. Above that would be retaining degrees of mission performance. The Navy has plenty of experience designing for these types of requirements.

Deception: As stated earlier, it's increasingly difficult to hide surface vessels from the array of sensors that can be employed to detect, identify, and track them. It is also extremely difficult to win the cost exchange ratio battle against the range and density of missile threats that can be employed against surface vessels once they are targeted. Deception, in the form of decoys meant to emulate vessels could be very cost effective. They would certainly be unmanned vessels and would need to emulate or anti-simulate real warships. This is relatively easy to do, but still not cheap if only passive signatures are emulated. Emulating active signatures, for LPD/LPI radio frequency emitters increases cost, but also increases deception effectiveness. Beyond the use of deception to emulate individual targets in a formation, actual operations could be simulated as well. The U.S. has not embraced the widespread use of deception in general for a very long time. Presumably because it diverts resources from "real" capability. Against a threat with a formidable lethal capability the use of deception becomes much more cost effective and should be considered, including for surface vessels.

Directed Energy Weapons: I've been watching directed energy weapons, primarily lasers, be five years away from military applications for 50 years. Power levels, size, weight and power (SWAP) parameters and efficiencies have all improved over time. Warships provide a good environment for the volume, mass, input power, stability, and heat dissipation needed for high energy lasers. At this point, however, I'm still agnostic about the contribution they will make. Lasers, and the optical fire control sensors that aim them, are limited by atmospheric conditions like fog and rain–both common at sea. They require nominally a few seconds of dwell time on an incoming missile to defeat it, limiting how many engagements they can conduct during the time window of a large, coordinated attack. They may not provide actionable feedback on their effectiveness, making the decision to move to another target high risk. The threat has a vote, and can use combinations of hardening, maneuver, and tactics to limit the effectiveness of lasers. Microwave weapons have similar problems. I'm open to the possibility of including directed energy in future warships, but they will have to earn their way on by demonstrating their utility and resilience first.

Electromagnetic Weapons Launch: This is another technology that has been worked on for decades and for which naval applications should be attractive because of the volume, mass, and power that ships can provide or accommodate.[28] The concepts I've described could include this technology for long-range strike and for self-defense, but it is going to have to demonstrate its relative cost effectiveness over other options first.

Energy: Future military surface vessels as envisioned here, will employ the most efficient energy sources available for propulsion and for onboard systems when they are fielded. At this point I would anticipate the infrastructure to support refueling, including in all likelihood at-sea refueling, will have to be included in the concept. Small unmanned surface vessels can utilize non-traditional energy sources such as wind, solar, and wave riding for long and very long endurance missions, but with penalties in speed and maneuverability.

[28] Electromagnetic aircraft launch is on the new Ford Class Carrier which has now entered service.

Fast Attack Craft and Fast Inshore Attack Craft (FAC/FIAC): This is primarily a coastal threat to large warships and commercial traffic operating in confined areas or near shore in general.[29] Swarming small vessels like this provide a potential way to attack capital ships cost effectively. Any vessels in the concept that would operate where they could be subject to this sort of attack would have to be armed with the means to defeat them. A modular approach to providing that capability when needed seems like a reasonable approach. The degree of human control, on board or remote, of such a defensive system would need to be flexible depending on the circumstances. I do not envision a swarming small craft option for the U.S. because of the problems associated with delivery of those craft to where they are useful and because they would be essentially all expended when used. Delivery is necessary because of their limited ranges. Also, either they wouldn't survive or their trackable return to the "mother ship" would likely be fatal to that vessel.

Intelligence Integration: The C3BM architecture would need to flexibly integrate threat and other relevant intelligence for a wide range of sources, including air and space in particular. Organic sensors would only provide a fraction of the information associated with attacks or targets for strike. On board generated information might be sent to a shore-based node for inclusion or integrated with information sent from shore as it arrived. In general, however, operational and tactical intelligence integration would take place under human supervision where it made the most sense to integrate the data—generally not on the warships, even the manned warships if they were part of the formation. For defensive purposes, the necessary intelligence, processed to meet on board and group tactical automated decision needs, would be pushed to the warships, along with governing rules of engagement. Until engagement planning needed to occur, the ship or formation would only need limited information to carry out instructions. Once engagement planning was necessary, early engagement (launch on remote) instructions would be sent. At some point, as threats closed in time and distance, organic sensors and organic BM would begin to control engagement decisions. For strike missions, intelligence would generally be integrated in nodes ashore and strike orders would be passed to the warship formation. Throughout the architecture, edge processing of raw intelligence sensing should be emphasized to limit data flow (bandwidth) requirements.

Interoperability: The Navy has a concept of an integrated several hundred ship collective naval capability with our allies. That's a sound concept but achieving it with the concept I've described will take unprecedented degrees of interoperability. At some point our partners might adapt similar operational concepts to the one I've described, but for the foreseeable future one can expect a mix of more traditional allied vessels and the types of autonomous vessels I've described, possibly together with manned U.S. vessels. We will need to be technically interoperable with our partners to be effective. The U.S. is constantly conducting naval exercises with friends and allies around the world. We would want that practice to continue for several reasons. I expect interoperability would be achieved incrementally. The first step would be some integration of individual or small

[29] Interestingly Thomas Jefferson once sponsored a similar concept for US coastal defense – swarming small gunboats with a single cannon operated by part time militias. It was tried in the War of 1812 and didn't work out very well—none of the gunboat commanders wanted to go first against a British ship of the line with a full broadside available.

numbers of allied vessels with the warships I've described. As now, we'd need means of intelligence sharing and integration of the allied vessels into U.S. formations or at least the ability to communicate, share data, and operate cooperatively. Past efforts to achieve this sort of integration have had mixed success at best, but that is as much a matter of prioritization and command attention as it is technology.

Humans in The Concept—location, roles, and support for: The critical humans in the concept are the ones in the command organization, either ashore or embedded on a ship in the formation, overseeing the operations of the force and providing executive control. I did provide for a small C3BM team on a subset, or even on each, of the warships as an option because the overhead cost was low and one could envision cases, especially in peacetime, or tense situations short of conflict where having some humans on-board would be of value. There would also be humans involved in remotely overseeing the continuous operation and the nearly continuous updating of the software associated with the operating and combat systems on the ships. Embarked humans would need to have all necessary life support on the ship.

Hypersonic Weapons: They would be included based on cost effectiveness. The ships could be designed to host boost glide or hypersonic cruise weapons. I'm not fully persuaded these weapons will be cost effective in large numbers for strike missions against the target sets of interest to U.S. commanders. They do have better penetration capability against current defenses, and they have shorter times of flight than transonic cruise missiles, but one has to weigh the costs and trade-offs between these and other options for the target sets of interest. Intuitively I believe that some number of these weapons, delivered by some means, makes sense in the U.S. inventory. I'm not persuaded at this point that those numbers are large, or that surface ships are a needed host for them.

Legal Constraints: There are a number of legal constraints that apply to the overall concept and some that apply to the warships I've described. I don't see anything unique in the sea surface domain that would be especially problematic. COLREGs compliance was described elsewhere. Humanitarian and law of war provisions would apply to the use of force as in other domains. There are some unique maritime legal considerations, salvage law, waste disposal, other environmental regulations, marine mammal protection, fisheries, customs, quarantine, and piracy for example, but nothing that precludes the concept that I think is unworkable or that the Navy doesn't address routinely.

Loss of Contact/Control by Echelon: This is an area where reliability and resilience are particularly important and where off-board sensor based situational awareness is an absolute necessity. The ability to track a vessel's location should be multiple-redundant and failsafe. The ability to determine status and take basic control over maneuvering should be almost the same level. Default behaviors implemented on board in the event of loss of external communications or partial organic system failure should be tailored to the situation and both monitored and updated continually.

Marines: Large scale amphibious operations aside, Marines are often embarked on warships to provide a contingency capability and to provide physical security against some threats. For the core escort and strike missions the concept was designed for, they aren't necessary, but the

flexibility to have a support module to embark a squad size or even somewhat larger unit of Marines on board would be an option that could be designed in.

Operational Planning and Rehearsal: This would take place at the C3BM nodes, likely ashore. Rehearsal would be virtual of course. Prior to a deployment or operational mission planning, war-gaming, alternative analysis and virtual rehearsals could all occur in a synthetic environment, but if would certainly make sense to include the live onboard systems "in the loop." During operations of any type, planning would be updated continuously as the tactical situation changed.

Organic Aviation: An option should be provided to embark organic aviation. I don't believe every vessel should have organic aviation for every deployment of mission, but it would be a valuable asset to have in a number of circumstances. Organic or at least warship-compatible unmanned aircraft could extend local high-resolution surveillance for various missions, provide for evacuation and support to vessels with humans embarked, and provide an extended range communications link. In some situations, they could also be armed to counter relevant threats. An advanced design roughly in the category of the Fire Scout MQ-8C Model seems about right. A tiltrotor or other advanced vertical take-off option would be possible as well. Such a system would have to be reliable enough to operate without continuous onboard support and it would have to be capable of being refueled or recharged onboard autonomously.

Physical Security: Some security would be provided by the basic design which should defeat unauthorized entry for low end threats. Non-lethal effects could be used to provide additional deterrence. Anti-piracy techniques might be relevant in some cases. I wouldn't rule out remotely activated and operated, or even in some circumstances autonomous, lethal defense mechanisms. In port, more traditional security can be provided as needed. Underway, the suite of capabilities described here could be activated, with degrees of severity depending on the threat and the situation.

Port Facility Support and Pilots—Overseas Basing: In a world in which autonomous commercial shipping comes and goes, I don't see a fundamental obstacle to overseas basing. The vessels would have the provision to be optionally manned and could take a pilot aboard if required to enter a port. More likely, as I expect for future commercial vessels, the pilot function will be performed remotely without the need to board the vessel. The same could be done for the warships in the concept. Any time one of the envisioned vessels entered a foreign port it could be met by humans (Navy or contracted) for in-processing, assessment, arrangement of needed maintenance, refueling and rearming, and to provide physical security.

Reliability: This may well be the biggest obstacle to realizing the described concept. Redundancy can help, but some shipboard systems cannot be redundant because of their size and/or cost. Many critical supporting systems are made of components or assemblies that can be changed out at sea from a spares inventory carried aboard, but not on an autonomous ship. I do not envision a general purpose highly flexible electrical, mechanical, or hydraulic "repairperson robot" any time soon. The consequence of an unrepairable casualty at sea can be catastrophic, causing a return to port or the need for a salvage operation with off-board assets. Of course this is somewhat true for manned ships also, but spares for high failure rate components can be stored aboard and installed as needed

at sea on manned ships. That won't be the case here. Humans are very good at replacing complex parts—this function isn't going to be automated in a general way for some time, so high reliability is a necessity. Fortunately, a lot of progress is being made in this area, especially for commercial electronics and other components where the market rewards high reliability. Unfortunately, a lot of shipboard parts don't meet this description.

Replenishment at Sea: Refueling at sea is likely to be a necessity and would have to be automated.[30] With current technology an autonomous or minimally manned vessel of the size envisioned would have an unrefueled range of several thousand miles. That isn't enough. I believe this function could be automated, but a lot of work will have to be done to demonstrate it can be done effectively and consistently in a reasonable range of sea states.

Requirements Creep: Conscious attention should be placed on avoiding cost imposing marginal or low return on investment requirements. The natural tendency in all domains is to add more and more requirements to the design until the concept crashes from its own weight. A lot of the items on this list are good examples of potential requirements creep. The whole point of the concept is improved cost exchange ratios over current systems.

Responsive Threats: The threat spectrum here isn't significantly different than it would be for new manned warships. The potential Achilles heel of cyber or EW attack on an unmanned ship would be very attractive. Just isolating the ship from its C3BM system would have a crippling effect if it prevented integrated multi-vessel extended range operations–for either air and missile defense or strike applications. We can expect the threat missiles to achieve longer ranges, employ countermeasures like decoys (in the case of ballistic threats) and self-protection jammers, adapt maneuvering and collaborative tactics, and use attack structures tailored to the defending force. When dealing with a thinking, competent, and well-resourced adversary, we will need to be at least a step or two ahead in analyzing potential responses and either designing for them or making provisions for growth paths to respond when they materialize.

Salvage/Recovery: Bad things can happen to ships necessitating salvage or recovery. One provision to consider is the idea of recovery of one autonomous warship by another. The ability of salvage and recovery teams to come aboard and deal with a range of possible casualties should be provided for in the design. This function won't be fully automated anytime soon—although small autonomous vehicles could do some aspects of this function.

Single Points of Failure: This is a subset of the reliability requirement, but it specifically addresses nodes or functions that are essential to operations and forces consideration of backup or lesser included capability alternatives (graceful degradation) and a means of reverting to them as necessary. The autonomous operating system for the vessel and its principal weapons systems and sensors as well as the C3BM architecture are all critical to mission success. This can't be done for every function in the so-called kill chain, but it should be part of the design process.

[30] It depends on the unrefueled design range. Ships in the class we are talking about here probably couldn't conduct a subset of needed missions (Pacific transit plus operational maneuvering as needed for example) without refueling.

Stealth: There are different types of stealth for different threats. Defeating even a subset of the adversary's sensors can have value. It may not be possible to hide the presence of a vessel from some types of observation, space-based wake detection for example, but other aspects of the system, the fact that it's a warship, or the ability of a threat seeker to detect the ship or its most vulnerable area might be thwarted. Stealth in conjunction with deception, discussed earlier, can have symbiotic affects that merit the inclusion of stealth in the design. Operation in a passive mode was discussed earlier. Low probability of detection and intercept emissions through various techniques can contribute significantly. Reduction in radar and optical signature or creating confusion about identity can have value also. The Navy has worked on each of these approaches, but the overwhelming nature of the threat is pushing us toward the need for concealment in lieu of active defense as a much more significant contributor to survivability. The design should reflect this reprioritization.

Training, Experimentation, and Testing: One virtue of unmanned sea surface concepts is that there is no need to keep ships at sea on a continuous rotational training cycle to maintain the proficiency of the humans who tend to lose competency unless it's exercised frequently. Computers don't forget. That doesn't mean there should be no exercises or live training, but the need can be significantly reduced, and much more can be done through virtual and constructive means. Allies can be involved in this as well to improve interoperability. Some traditional testing—shakedown deployments, trial Bravo for new construction, etc.—would still be required.

Unattended Sea Surface Sensors: Unattended sea surface sensors are generally slow moving or drifting, but they can be proliferated economically, be expendable, and have high utility. They can be made very difficult to detect. The options include wave gliders and sail drone concepts and drifting buoys. These systems can also be used by adversaries as part of their overall ISR suite, and in some cases (such as choke points or sea lanes) they can be weaponized as well and be very cost-effective mines. I can see both the U.S. and its adversaries using these systems, possibly extensively. As their use increases, this will levy significant requirements on ISR systems in space, air and sea-surface domains and create a demand for cost effective neutralization mechanisms.

Weapons Mix: For the surface warships in the concept, the design should accommodate flexibility in weapon load out for the operational mission, using common interchangeable weapon modules where possible. The mix could include anti-air weapons, conventional and hypersonic strike, anti-ship missiles, and anti-satellite weapons, remote delivery of unattended sensors, and possibly other weapons. It would be highly desirable for these modules to be replaceable a sea.

Weather Implications and Forecasting: I don't foresee any novel weather-related design requirements different from those for current systems. It might be possible to push for higher sea state capabilities and relax some of the current motion and stability related requirements for human operated warships in those cases where the vessel is operating unmanned and autonomously, but I doubt that would accomplish much. With regard to forecasting, the needs would be similar to those for current operations, with even more precise forecasting desirable. Space-based systems would be needed to provide this support.

Other Needed Military Functions

Amphibious Operations: Traditional amphibious assaults against prepared peer competitors are problematic because of the vulnerability to precision weapons of the transporting surface ships and landing craft and the relatively slow pace at which any amphibious landing can be conducted. Smart, or even traditional, sea and land mines compound this problem. Just the process of loading, deploying and navigating landing craft ashore can take hours, and the deploying ships must be within relatively short-range of the landing sites, even if they can be held over the horizon from shore. The Marine Corps has tried to speed up this process with greater use of aerial delivery and faster landing craft, but the fundamental problems have not been overcome. The Marine Corps has also attempted to develop doctrine and concepts that increase the probability of successful amphibious assaults, and most recently the Marine Corps is shedding some of its heavy and less transportable equipment, such as tanks and towed artillery. Despite these efforts it's still a major undertaking to get Marine units ashore and importantly to support them after a landing. If the supporting ships cannot survive or remain on station to support the assault force it will likely be defeated, whether it is composed of primarily autonomous systems or more traditional ones. As a result, the best alternative for forced entry from the sea may be to have the capacity through air delivered weapons, enabled by air and space-based ISR and C3BM, to neutralize defenses so the assault force is weakly opposed or unopposed. "Going where they ain't" is another theoretical option, but difficult if not impossible to achieve given the ubiquity of sensor systems to detect an assault force and the availability of long-range anti-ship precision weapons with target detection and selection capabilities. Suppressing the ground mobile long-range precision missiles that would be used to target amphibious shipping would be a daunting task, but it isn't unthinkable. It would be desirable or even necessary to establish dominance in the air and in space prior to attempting an amphibious assault. Once that is accomplished, one can envision a highly autonomous suite of systems, including those discussed in the land domain section and compatible transport shipping as the basis for a forced entry ground force. The transport shipping would be designed specifically to support the rapid movement of a UGS and UAS force, as described in the land domain section, ashore. The best delivery means, because of their speed, would be aviation assets as opposed to landing craft. The organic UASs in the land domain concept would be the "first wave" ashore and would eliminate short and intermediate range threats and provide over watch for the subsequent air delivery of their hosting UGVs ashore. Once the full force was ashore it would function identically to the land domain concept.

Anti-Submarine Warfare (ASW): Sea surface assets can be vulnerable to attack by submarines using torpedoes or stand-off cruise missiles and ballistic missiles. Surface vessels and their organic aviation assets also have a role in ASW. As I'll indicate in the next section, I believe the ASW role overall is moving toward air and space-based as well as undersea systems. Nevertheless, surface warships can carry both sensors and weapons that can be useful in ASW operations. Surface vessels must be able to defend themselves and other assets from missile and torpedo attack, whatever the source. Defense against torpedo attack is best achieved by attacking the launching platform, submarine or otherwise, but I would continue the research effort to develop surface ship

self-defense capability against torpedoes. I can't predict if it will be successful over time, but it is worth pursuing and has a chance of success.[31]

Counter Piracy and Counter Narcotics: These are law enforcement missions and should not be major design drivers for naval warships intended to prevail against peer competitors. The concepts defined above could contribute to these missions and would be expected to do so.

Blockades and Embargo Enforcement: If the missions involved stop and search, some manning and even a Marine or other armed boarding party module would be desirable. The offshore cutter class design would be suitable for this function as well. If the situation was hostile and the blockade was lethal, the calculation would be different. Unmanned systems with off board tight C2 could be effective. In that case, space and airborne capabilities might be a preferred choice.

Disaster Relief / Humanitarian Assistance: The U.S. military does these missions with some specialized assets, like hospital ships and small deck carriers effectively as an inherent capability. My view would be that we shouldn't buy military assets specifically for these missions, but we should certainly use the military assets in the inventory where they can be effective for this mission. I would expect the U.S. to have relevant assets for this mission for the foreseeable future, but perhaps not in the current density.

Freedom of Navigation Operations: The autonomous vessels in the concept could certainly do these missions, but if unmanned they might be a tempting target. This is another, but not compelling, reason for optional manning, even in small numbers.

Mine and Counter-Mine Warfare: Future surface domain concepts overall should include sea mine options, but they would probably be delivered covertly by undersea systems or possibly by air. I'll discuss smart mines in the undersea section. Countermine warfare is an issue for amphibious assault forces and when friendly shipping (military and commercial) has to transit areas where mines can be emplaced and be cost effective–choke points, for example. The undersea domain is an extremely difficult countermine environment. The potential for false alarms, the opportunities for concealment, increasing smart mine options, and the relative ease of providing decoy mines to delay and increase the cost of clearing are all problematic. The U.S. Navy and others have pursued autonomous vehicle-based solutions, deployed from surface ships primarily, and airborne sensors for some time with at best mixed success and some failures. This effort will continue and can be increasingly unmanned and automated, but I will be surprised if it ever achieves high confidence rapid mine clearing capabilities. Reliable mine field detection (vice individual mines), avoidance, and relatively slow clearing processes, all done autonomously, may be the best we can expect.

Naval Bombardment/Fire Support: The warships in the concept could provide this with missile systems, but with less volume of fire than gun systems for a similar sized vessel. Gun systems aren't out of the question, either electromagnetic launch or more conventional. They would have to earn their way into the concept through competitive cost effectiveness. Against a peer

[31] Anti-torpedo self-defense systems in the U.S. have been attempted but have not been successful to date. The US Navy is reported to have canceled its program. The German Navy is continuing its Sea Spider program and has reported a successful test.

competitor, the survivability of any surface vessel providing fire support to forces ashore is questionable, but in many operational scenarios it could be cost effective, particularly against threats where the anti-ship kill chain had been suppressed (see the amphibious operations discussion above) or in something akin to an "artillery raid" concept for ground forces.[32]

Regional Missile Defense: Aegis-equipped ships currently provide a contribution to regional missile defense of assets on shore. The ability to move these ships to a given theater, and to the proximity of protected assets or to an optimal point from which to conduct intercepts against a given threat, provides some useful operational flexibility. The envisioned surface warships could perform this function, and to the degree which their presence can be concealed, they could make a threat attack planner's problem more difficult and higher risk. Their mobility would also improve their survivability once they start conducting intercepts.

Special Operations: Presumably some types of special operations conducted from the sea, such as raids and support to covert operations of various types, would still be needed. The surface warfare concept wasn't designed for those missions and specialized surface or subsurface vessels for those purposes might still be needed. We won't be fully automating these complex functions any time soon, and some of them require human-to-human interactions. Some subsets of special operations could be conducted with automated systems, however, such as covert delivery of support to insurgent groups or loitering covert weapons for surgical strikes on specific targets.

[32] Something similar has been proposed for aircraft carriers–short excursions within the range of missile threats. Given how long carrier operations take and how detectible they are, this seems like a highly risky proposition to me.

Warfare Domains – Sea Subsurface

Introduction

The subsurface domain was identified during the work on Competitive Strategies and the Third Offset Strategy as one of the few areas—maybe the only one—in which the U.S. retained a substantial advantage over its near peer competitors. The U.S. advantage is largely in the areas of stealth (quieting primarily) and sensing. While submarines do carry some defensive countermeasures to defeat attacks, they are very limited. Submarines achieve their survivability largely through not being detected. Over the modern era, efforts to improve active and passive acoustic detection have received the most attention, with heroic efforts to improve submarine quieting and resilience against active sensors through sound absorption and other techniques. There are two problems with relying on stealth so heavily for survivability: first, it can be fragile—once it is lost, submarines become very vulnerable; and second, it limits the things a submarine can do operationally.

For years major powers have worked to defeat submarine stealth. Submarines are fairly large metallic objects with a variety of signatures—acoustic being the one that has received the most attention since submarines came into existence.[33] Because of the U.S. reliance on the submarine-based leg of the nuclear triad, submarine survivability has been of grave concern for several decades. It is beyond my classification level in this paper to write in much detail about the current state of ASW technology. In general, there is a recognition that hiding submarines is becoming harder as sensor technology, the ability to detect novel signatures, and the capacity to pull signatures in general out of the noise all improve. Quantum sensing, artificial intelligence data analytics techniques, machine learning, and the proliferation of sensor systems at sea and elsewhere are working against the continuing efforts to improve the concealment of submarines. I can't comment here on the precise state of that competition, but time and technology are not on the side of the submarines.

Like modern surface combatants, submarines are big, expensive, and slow. When submerged, their ability to sense beyond the immediate environment is very limited. A Virginia class attack submarine is 400 feet long, weighs about 8,000 tons, and has a crew of 135. Unlike surface combatants, submarines are relatively survivable, until they try to go fast or to fire off weapons or to operate at or near the surface. Speed means creating much more noise in the water; firing weapons—either torpedoes or missiles—creates a large signature. Coming to periscope depth to collect information significantly increases detectability. Unlike surface combatants, submarines also have almost no capability to defend themselves once they are detected.

The threat to submarines, in addition to other submarines, includes fixed and deployable sensor systems have been employed to geolocate submarines, particularly as they transit confined waters. Detecting a transit provides queuing for more localized sensors and for other submarines to track

[33] I've spent part of my career on the anti-submarine problem, going back to the Air Defense Initiative in the 1980s which focused in large part on countering Soviet submarines that could launch nuclear armed cruise missiles from off the shores of the United States.

the detected submarines. It's one thing to search an open ocean area for a submarine that may or may not be there. It's considerably easier to stay on top of a known submarine once it's been detected and geolocated. If one has the freedom to operate them, airborne ASW platforms, like the shore-based P-8 with deployable sonobuoys and other sensors, and the ship-based MH-60R helicopter with a number of sensors, provide a significant threat to current submarines. It's been a truism that someday submarines will become detectable, and their relative security will be fatally compromised. To most observers that day has not come, and it always seems to be a few years away, at least. As I look at emerging technologies such as those mentioned above, I'm convinced we cannot count on the long-term viability of submarines as we currently build them. In 2016, I asked the then-CNO, a submariner, what his views on this were. I won't repeat his answer here, but it was not reassuring. If we take it as a working assumption that current large, crewed submarine designs and concepts will become vulnerable to detection and attack (at least when operating in waters of interest within 1,000 miles of adversary coastlines) somewhere in the 10-to-20-year window for this paper, where does that leave warfare in the future in the undersea domain?

Considering the potential for unmanned undersea vessels opens up some significant design trade space but also brings some challenging operational problems. The Navy has been experimenting with undersea autonomy for some time. Until recently, this generally took the form of small Unmanned Undersea Vessels (UUSVs) that could be deployed from surface vessels, through submarine torpedo tubes, or from the decks of manned submarines. Countermine operations and local surveillance and reconnaissance missions have been explored to varying degrees. Today the Navy is also entertaining new concepts for what it calls Subsurface and Seabed Warfare (SSW), a phrase that captures the mix of manned and unmanned undersea vessels, fixed and mobile sensors, and seabed infrastructure for communications, power, and other uses. This is promising, but the potential exists to go much further. Most recently, larger experimental designs with longer range surveillance or with mine and sensor delivery missions have been developed.[34] For these, and any unmanned undersea system, a major issue is command and control, simply because of the physics associated with undersea signal transmission. This can be mitigated in various ways, but with some associated penalties in detectability and mobility. Let's see what operational capabilities might be feasible in the foreseeable future.

Operational Concept

I'll assume we are primarily interested in defeating enemy submarines and surface ships using assets that operate in the undersea domain.

If one accepts that reliable long endurance UUVs are plausible, and that some degree of lethal autonomy in the undersea realm is acceptable, then it opens up some interesting possibilities. Both of these developments are essentially at hand, technically at least. The first mission we should

[34] Most notably the ORCA XL-UUV, which Boeing and Huntington Ingalls are now building five of for the Navy. At this point these are experimental systems, and the Navy is working to determine what payloads and operational missions would make sense for the platform.

consider in this domain is ASW—defeat of an enemy submarine force. Traditionally submarines are thought to be the most effective anti-submarine platform and torpedoes the most effective anti-submarine weapon. (I'd argue if they could be successfully built, wide area airborne sensors or air delivered sensors from fixed wing and helicopter platforms together with air delivered munitions would be much more cost effective, but let's stay in the undersea regime for now.) What would an ASW operational force look like given these developments? We need to accomplish three operational tasks; detect and localize the enemy submarines or submarine force, establish targeting quality information on the enemy submarines, and attack the detected submarines successfully. We need to do all these tasks while achieving a favorable cost exchange ratio.

At the start of a conflict an opponent may have some submarines at sea and others in port. It would be highly desirable to at least approximately geolocate each enemy submarine and to keep it under surveillance continuously, from prior to the start of a conflict until the submarine was destroyed. I won't go into the potential to do so from space or the air here, but that should certainly be considered and will be discussed as a multi-domain consideration. For now, we'll hypothesize an ability to have multiple hunter killer UUVs on station to track any enemy submarine, either from the time it leaves port (both prior to and during a conflict), or as it transits a known choke point, and to maintain that track indefinitely. The basic operational organization I envision is a small group of nominally three medium-sized UUVs that can operate together to defeat and destroy an enemy manned submarine. The unmanned and autonomous platforms needed to do this would be much smaller (and therefore much cheaper) than manned submarines, but they would need the capability to move stealthily. Sensors on this UUV would be primarily passive to avoid detection, but could include active sensors, on at least one of the UUVs, to support engagements. In situations where the enemy submarine's location or even presence was uncertain, one basic scheme would be to have one of the UUVs go "active"—transmitting sonar signals that would provide bi-static and mono-static information about the threats' location and movements. This active transmitting UAV would be effectively sacrificial as it would expect to "draw fire" from the target submarine. All three UUVs would simultaneously engage the enemy submarine, achieving a favorable exchange ratio of no more than one UUV lost to destroy the manned enemy attack boat—a much more valuable asset than the UUV.

It could similarly be presumed that a friendly UUV stationed near an enemy coast would be destroyed fairly quickly once it had attacked a transiting enemy submarine (or surface ship). If hostilities had already started, then engagements could be conducted as soon as an opponent's submarine attempted to leave or enter port. If not, then our unmanned platforms could remain passive, probably concealed on the seabed (effectively as dormant smart mines), until activated at the start of hostilities. A necessary feature would also be the ability to reliably and clandestinely receive off-board activation instructions at the start of hostilities, possibly to report engagement results, and to receive relocation and new mission instructions. Continuous human C2 is not assumed or required.

Building Blocks

Experimental UUVs roughly in the right size ballpark are already being built. The Navy refers to them as Extra Large Unmanned Undersea Vehicles or XLUUVs. Mine delivery, ocean surveillance, reconnaissance, and intelligence missions are near term applications and there have been recommendations they be used for unmanned Tomahawk cruise missile launchers and mine delivery vehicles. The extension from these limited experimental systems to a collaborative lethal autonomous ASW capability is a matter of integrating the necessary sensors and weapons and command and control capability and gaining confidence in their reliability and effectiveness. This is not a huge leap. Exploring the realism and operational potential for this concept will require multiple prototypes that can operate as a team in the manner described above. For operational assets, there are a number of design trades that will have to be conducted to balance cost and the range of features needed to implement the operational concept. These problems are not trivial, but the most significant may be achieving the confidence level needed to support engagements, and achieving the range, data rates, and reliability needed for communication among the small unit of collaborating submerged UUVs that is envisioned. Modular designs that enabled multiple mission load outs would be attractive and improve the utility and cost effectiveness of the UUVs. This is the intent of the Orca XLUUV program already. As in other unmanned systems and domains, losses associated with attrition are expected, so cost will be a major driver. These systems would have to be acquired in significant numbers, but their cost should be a fraction of a manned nuclear attack submarine.

In this concept, the XLUUV serves as the transporter and launcher. The projectile for ASW would be a torpedo which would be an evolutionary version of current systems. If justified by trade studies, the UUVs in the concept could be designed to be launchers for projectiles for other missions, ASuW and Strike especially. I'm slightly skeptical of the utility of this approach, but it is worth exploring.

Complexities

Fundamental Operational Needs

Command, Control, Communications, and Battle Management: As noted earlier, continuous communications with manned installations ashore or on surface ships would be problematic during submerged operations. There are ways to use deployable buoys and other devices to achieve this in some circumstances, but not as far as I know during tactical operations. Receiving commands and revised rules of engagement this way is relatively easy, followed in order of difficulty by low data rate acknowledgements and status reports from the UUVs. Detailed status reporting and data intensive intelligence reports are most stressing, but can be provided for, possibly after moving to a less threatened environment. This seems to be the Navy's current intent for the Orca program. In any event, both individual and small groups of UUVs would have to conduct submerged operations without continuous human control. I don't see this as a showstopper for the concept, but it is a critical operational need. For tactical operations involving collaboration among multiple UUVs, local undersea communications must be adequate to support tactical behaviors. If one UUV is

using active sonar for threat detection, that UUV can use active acoustic signals to inform the others in the collaborative team of its location and to provide information on the threat environment. Laser systems would be more secure but are sensitive to the undersea environments and are range limited. The active UUV platform takes on the role of local central node and all other platforms orient around that node autonomously.

Cross Domain Considerations: The focus of the concept is ASW, which is a heavily cross domain mission. Airborne assets, both fixed wing like the P-8 and rotary wing like the MH-60R play a major role in ASW. Surface ships with associated aviation can play a role as well. I would expect these roles in ASW to continue, but transition to unmanned platforms. I would also expect space-based sensors to play an increasing role in ASW. The envisioned XLUUV assets also have roles in other domains beside undersea. Obviously ASuW missions would be viable and cost effective. Submarines have a traditional mission of interdicting enemy shipping—military and commercial—and the XLUUVs could contribute to that mission. Large UUVs move slowly compared to surface ships.[35] As a result "ambushes" at choke points or harbor approaches and engagements are move achievable than unconstrained open ocean ASuW. Torpedoes have multi-domain, surface and subsurface, applications, but relatively short-range. Anti-ship missiles launched from XLUUVs would provide a much more flexible surface ship engagement capability and improve the survivability of the launch platform but reduce the inventory for the ASW mission. The UUVs in the concept will depend on off board long haul communications for command and control. Space is the most efficient way to meet this need, but airborne relay options are also possible.

Logistical Support: The UUVs in the concept would have ranges of several thousand miles and long endurance. Orca's reported range is 6,500 nautical miles and it has an endurance measured in months. As a result, logistics support would be provided from ashore in secure locations, although the potential for replenishment at sea is certainly available. There would be some operational value to provisions for munitions and other expendables replacement forward, given the slow transit speeds expected, but the survivability of the logistics vessels would have to be high enough to justify doing this.

Tactical Mission Variations: Depending on how successful modular designs are, and on the planned load out of munitions, XLUUVs could perform a variety of functions, most of which do not require tactical real time collaboration. These include ISR, mine delivery, EW and possibly cyber. Mission variations that involved alternative payloads would have to be planned well in advance, however. Single platform or non-collaborative mission assignments are certainly possible and that's the first capability likely to be fielded. At the other extreme are many-on-many mission situations (ambushing an invasion fleet for example), that would require large deployments and reward higher scale collaboration for more efficient target allocation.

Target Identification / Collateral Damage Avoidance: Location and threat classification, as a submarine or capital warship, would be adequate during hostilities and in an area where there was

[35] Orca's reported transit rate is about 3 knots.

known to be no friendly or neutral shipping. In those cases, rules of engagement could be relatively permissive. In other situations, higher or much higher confidence levels would be needed and would have to be verified through extensive testing. Even in a situation with loose rules of engagement it would be useful to have target identification, through acoustic signature alone say, adequate to support autonomous decisions favoring high value target engagement.

Design Requirements and Considerations

Active Defense (Counter-Torpedo Defense): The XLUUVs in the concept are not small (over 50 feet in length) and valuable enough to consider some limited self-defense provisions including active defense measures and expendable decoys in the design. It's a cost benefit trade-off worth considering, but the results are not obvious, either from a feasibility standpoint or for cost effectiveness. If these platforms are intended to be attritable, or if a subset of them are sacrificial it may be hard for these systems to earn their way into the concept.

Anti-Tamper: There is a high probability the UUVs in the concept would fall into enemy hands at some point. Either the wreckage of defeated systems would be recovered or UUVs could be trapped in some form of disabling netting, including commercial fishing nets (although the Navy's current XLUUV design requirements include a provision to avoid this threat). Anti-tamper provisions would govern all of the sensitive systems aboard, especially weapons, secure communications, and autonomous behavior control.

Communication: At the surface or with the assistance of a deployable buoy, state-of-the- art secure radio frequency transmission to space-based or airborne assets would be required. In some environments, commercial SATCOM could be used. Tactical acoustic or optical communication for undersea operations and tactical collaboration were discussed earlier.

Confidence in Automated Behaviors: The undersea environment is a relatively benign environment for transit–there isn't much to bump into as long as one avoids the seafloor and stays at a reasonable depth. Surface or near-surface operations are similar to those for USVs. Individual XLUUV tactical behavior is relatively straightforward. The greatest challenge will be automated collaborative tactical behaviors, both the coordination of attack tactics and the avoidance of fratricide.

Cyber and EW: The XLUUVs in the concept could conduct EW missions—collection in denied areas especially. They could also serve as a node for wireless cyber insertion into commercial or even military networks. Specialized payloads or modules could be acquired for these purposes.

Deception: Concealing the XLUUVs until they conduct engagements is essential. They should be designed to remain passive until energized by the presence of threat signatures or as ordered. There would be operational value in providing false XLUUVs as both decoys where real XLUUVs are concealed and to very cheaply influence enemy behavior where they are not deployed.

Deconfliction: This is a design requirement, but I don't think this is a major problem for the ASW mission. The targets tend to operate individually and are high value relative to the weapons the XLUUVs would employ against them. We can probably afford to accept a modest risk of waste of

some weapons in this case and it may well be preferable to engage a given submarine or even surface ship with multiple threats. If these platforms were used for ASuW, against an invasion force for example, deconfliction would be a greater concern in the design.

Energy: UUVs will have to be designed for adequate range to perform their missions, but that can be achieved with current technology. More efficient sources of energy are likely to become available in the future. It is also conceivable that refueling during an extended mission could take place.

Fixed Detection and Tracking Acoustic Arrays: They can certainly have a role in the concept as early warning and cueing sensors as they do now. Covert deployment in locations of operational interest is important to deny defeat of these arrays by adversaries. Similarly, the U.S. needs to have the means to locate and disable adversary arrays, preferably covertly. UUVs can be employed, in peace and wartime, to serve these ends.

Humans—Role of and Support To: The humans in the concept are remote overseers of the XLUUVs. They provide operational guidance, policy, and force management, but generally not tactical control, from a secure enclave remote from the XLUUV force.

Intelligence Integration and Dissemination: The concept envisions small groups of operational platforms with limited communications operating at extended range for long periods—months. In this circumstance, intelligence integration and dissemination will occur under human supervision at a secure headquarters. The deployed XLUUVs would usually only need low data rate inputs. On some occasions, however, updated data files (threat signatures, for example) and updates to onboard software (signal processing algorithms, for example) would need to be transmitted to the XLUUVs. This could be accomplished through several alternative means and could involve movement of XLUUVs to more RF secure locations temporarily. In any event, it is a design requirement.

Interoperability: I don't see a firm requirement for the XLUUVs to operate with allies. Avoiding fratricide is a firm requirement, but can be achieved through coordination with the headquarters element instead of through direct contact with the XLUUVs. If the allies field similar systems, then closer coordination might be necessary, but even in that case I don't see direct tactical collaboration as a high priority.

Legal Constraints: There are a range of peacetime and wartime constraints that would have to be addressed, but nothing prohibitive as far as I know. Acceptable target identification to avoid collateral damage is the biggest and most obvious requirement. This function would have to be fully automated (within directed rules of engagement) unless continuous communications could be achieved somehow—something I don't foresee at this point. Once activated to conduct lethal operations, the XLUUVs are essentially mobile smart sea mines. They would be limited by anything that constrains that category of system. There are some restrictions on sea mines in Hague

Convention VIII and under customary international law intended to prevent indiscriminate damage to civilians and non-belligerents, but nothing prohibitive.[36]

Manned and Unmanned Teaming: This wasn't included in the concept I described because I didn't include manned submarines. The Navy is currently pursuing a Large-Displacement UUV (LDUUV) called Snakehead that would be deployed from a manned submarine and act as a scout for the manned submarine or perform other missions in conjunction with and in support of the manned submarine. The limitations on underwater communication between the sub and the UUV would limit the utility of the UUV. Its detection would also be a cue to the presence of the submarine. It's possible that this "scout" could penetrate into areas where the sub could not, but the XLUUV should be able to do the same, and it can carry much more payload than the LDUUV as well as operate from secure bases.

Mobile or Transportable Detection and Tracking Acoustic Arrays: These types of systems have been in use for some time and research on advanced versions conducted. I would expect work in this area to continue. There are concepts for deployable ASW sensor systems, active and passive, that could be used at choke points or to provide deployable and rapidly reconstitutable linear arrays for cueing when a submarine or large UUV transits. The cueing would enable airborne ASW systems or dormant UUVs to acquire, track, and engage threats efficiently.

Non-Acoustic Signatures: Work has been done for decades on a wide array of sensors other than acoustic. These include magnetic anomaly detectors, chemical sensors, bioluminescence, wake detection, and others. Signatures do exist in each of these and other physics regimes, but the problems of low signal to noise ratio and false alarm rates have generally limited their use, although some systems have been deployed by the U.S. and others. As sensors become more capable and processing capacity increases (think quantum sensing and AI enabled processing) there isn't much doubt as to where we are headed. Submarines as we know them are going to lose their stealth characteristic. It's just a question of how soon. I didn't assume that happened in this concept, but once it does, the undersea domain starts to have characteristics more like the surface domain and the value and utility of traditional undersea systems declines sharply.[37]

Operational Planning and Rehearsal: This is a problem for the concept I've described because of the limited communications options to UUVs and the long lead time to deploy assets on station. This isn't very different than the current situation, however. UUVs and any seabed systems will have to be pre-deployed or dispatched weeks ahead of any anticipated engagements. They would be able to receive updates periodically, and those could include operational planning guidance as needed. Rehearsals would be through simulations run in the controlling headquarters as part of the mission planning effort. For UUVs that would work as small teams in hunter-killer combinations,

[36] In the land domain, the U.S. has had limited success with developing Ottawa Treaty compliant (The US is not a party but has accepted some limitations.) smart mines with humans in the loop to authorize engagements. The cost effectiveness of these systems is questionable, and the military sponsors have had higher priorities. In the sea domains, mines, including smart mines, are not currently constrained by treaty and are in various countries' inventories.

[37] This event will have serious implications for the nuclear Triad, a subject outside the scope of this paper.

the algorithms for collaborative engagement planning and attack would have to be developed a priori and would be tested in live and virtual environments prior to deployment.

Peacetime Vulnerabilities/Physical Security: The UUVs in the concept, and any seabed sensor or smart mines included, would be at some risk of destruction, neutralization by other means, or adversary exploitation if detected prior to use. The design and operational concept are intended to minimize the risk of detection, but one has to assume it would occur at some time. A propulsion or control system failure can't be ruled out. There isn't much that could practically be done about in-situ destruction, or even some forms of non-lethal neutralization (nets for example). Anti-tamper provisions would be required for certain. Anti-access and/or self-destruction devices could be included in the design as well.

Recovery/Salvage: It would be desirable to be able to recover an inoperable UUV, but if the reliability is high enough, adding this provision might not be cost effective. For many reliability failures, a self-recovery option should be available. Towing by another UUV is problematic, but not inconceivable. In peacetime, recovery could be by a surface ship or "tender" designed for this purpose. If wartime recovery is desired, it might have to be through a specially designed or modified XLUUV built for that purpose.

Reliability: It has to be high enough for cost effective sustained operations, which means quite high. I don't see this as a major obstacle to the concept as existing submarines and UUVs have very high reliability and the technology to support the needed levels generally already exists. This does imply a very focused and conscious design effort in this area and enough testing to provide adequate confidence. The autonomous features of the platform would be embedded in software running on commercial hardware, and the reliability for both should be acceptable.

Responsive Threats: The immediate response would be to find ways using existing ASW systems, especially air and surface ship based, to negate the XLUUV threat, even if the odds of detection and the exchange ratios were poor. There would be attacks on the chain of control through cyber, EW, and kinetic attack means. Ground-based headquarters and C3BM facilities would be targeted if possible. There would also be an immediate change in the operational utilization of threat manned submarines, holding them back from risk especially. The first priority of an adversary would probably be its own coastal waters. Brute force efforts to find XLUUVs and negate them would be employed, expanding the use of expendable ASW sensors, both active and passive. There would be an acceleration of any ongoing or potential novel sensor approaches to improve detection and targeting. Finally, one could expect emulation—the building of similar capabilities to those in the concept. At least the first several of these responses should be addressed in the original design of the concept and its components.

Requirements Creep: Conscious attention should be placed on avoiding cost imposing marginal or low return on investment requirements. The natural tendency in all domains is to add more and more requirements to the design until the concept crashes from its own weight. A lot of the items on this list are good examples of potential requirements creep. The whole point of the concept is improved cost exchange ratios over current systems.

Single Points of Failure: Some redundancy could be provided, but for many systems on the UUVs this isn't possible. The greatest single point of failure threat may be adversary attempts to enter the communications loop to the UUVs and disable them or worse, take control. There has to be a robust communications design, which would likely include multiple link options, low probability of detection or interference modes, and a resilient low data rate mode.

Stealth: UUVs will be dependent on stealth, just as manned submarines are. They should have some advantage over manned submarines due to the absence of life support systems, human waste generation and disposal needs and overall reduced volume and machinery mass.

Unattended sensors: They can certainly be part of the concept and could be deployed by the XLUUVs. For some situations, such as outside of enemy harbors or at choke points, unattended sensors could be dormant and activated in either passive or active acoustic modes on command or as pre-arranged. They would be expendable, but a cost-effective alternative to losing XLUUVs in the same scenario. I could also imagine them being used in the open ocean as a cost-effective adjunct to the XLUUVs during ASW operations.

Other Needed Military Functions

Air Defense: I don't see this as part of this concept, but it's not totally out of the question. There have been concepts and experiments associated with air defense weapons that could be deployed from undersea platforms. A conceivable defense against a P-8 category ASW threat or an ASW helicopter is an automated air defense system (sensor and weapon) that could be deployed by one or more buoys to the surface if an ASW aircraft were known to be operating overhead. Of course, this confirms the presence of the UUV in the concept and it would provoke specific countermeasures to the air defense system.

Intelligence Collection: This is a traditional submarine force mission. Without going into detail, some of this mission could be performed by the UUVs in the concept, but some of it could not. The long endurance and loitering potential of the XLUUVs make them well suited for long periods of local observation and collection, without the risk of loss of life or detention of U.S. seamen.

Mine and Countermine Warfare: The XLUUVs in the concept could certainly be used as mine delivery platforms. That's a baseline mission for the existing program. They could also serve as transports for smaller UUVS for local mine detection, mapping, and neutralization systems.

Oceanography: This is another field in which submarines currently make a contribution through data collection. This work could also be performed by XLUUVs or other UUVs.

Seabed Warfare: Increasingly the seabed is used for communications links, for monitoring, sensing, and engagement using traditional moored or encapsulated mines and smart mines, and increasingly for commercial activity such as extractive industries. To the extent these activities generate targets of military value, they can be attacked by the XLUUVs in the concept.

Special Operations: Submarines support special operations by providing a covert transporter for Seal Delivery Vehicles and special operators with their equipment. Because they have no

provisions for human life support, the XLUUVs in the concept as they are envisioned cannot provide this support. It would be possible, at least for short duration missions, to include a module for this purpose, but I'm not convinced the utility is high enough to justify the cost. If this capability is a firm requirement, then some dedicated UUVs may be required. If delivery and retrieval is the limit of the requirement, it can be done with UUVs and probably with more acceptance of risk than for a manned attack submarine.

Strike Missions: The XLUUVs could be designed to carry cruise or ballistic missiles. Of the two, cruise missiles are probably much more cost effective because they could be launched from torpedo tubes without major modification of the XLUUV design. I don't see these systems as highly cost effective, but some number of them could be acquired as part of a larger force structure. The reason they aren't cost effective is the overhead cost of the XLUUV as a transporter for these weapons is relatively high. Weighed against that is the small number of weapons that can be carried, the risk to the launching platform once it starts to fire rounds, the possibility of discovery and neutralization before use, and the very long deployment and resupply times. This capability can have high operational value in some situations by destroying a few high value targets in the opening stages of a conflict, as a raid, as a pre-positioned deterrent, or as an enabling step for some follow-on operations. I wouldn't rule this out, but it will take some effort to justify it, especially at scale and relative to other options.

Warfare Domains – Air

Introduction

In the U.S., I believe we need to think about the air warfare domain as actually two domains. One is the short-range air domain and the other is the long-range air domain, in both of which strike and defensive as well as offensive counter-air are important. The need, and the opportunity, for long-range air operations only applies to countries with the resources and the geopolitical opportunity (or requirement) to conduct air operations at long-range. For the U.S., long-range conventional strike capabilities are cost effective because of their ability, from our unique geographic reality, to flexibly defend both our homeland and our global interests against any threat. If we were only worrying about defending the continental United States and having some retaliatory capability, we could limit ourselves to long-range offensive systems, but that isn't the case. We have close allies who geographically have no option but to engage in the short-range air domain. Our overseas allies do not have the favorable geography the U.S. enjoys, with friendly neighbors and oceans to protect us. We also have international interests we need to protect, located near potential adversaries. Finally, if we are going to conduct offensive ground operations anywhere in the world, we would need the ability to operate cost effectively in the tactical shorter range air domain environment where ground forces operate.

In both long- and short-range air domains, we also need to discuss air and missile defense. I include ground and sea-based air defenses, with the exception of close-range ground force or sea surface tactical unit self-protection systems, as part of the air domain forces. I discussed air defense in land and sea domains in the context of force protection primarily. Here, wide area regional and national air and missile defenses are a significant part of the struggle for control of the domain itself. The U.S. hasn't emphasized homeland or theater level surface-based air defense the way our potential adversaries have, but that doesn't mean we shouldn't or won't be forced to in the future.

In modern times, the U.S. has recognized the importance of air power in both short and long air domains and has emphasized investments in these domains. This has been true for decades, ever since WW II. Air systems come at a high cost, however. As Len Sullivan, the former Director of Program Analysis and Evaluation (the predecessor to CAPE) used to emphasize, "defying gravity is expensive."[38] It can also be decisive. In the future, control of the air will still be essential to success in war, even as the Space Domain takes on increasing importance. After the Cold War ended, the U.S. continued the B-2 and F-22 programs but drastically reduced the inventory sizes of both, significantly upgraded the F-18, and initiated the program that became F-35.[39] More recently, the AF initiated the B-21 medium bomber program. The debate about what comes next is now fully underway.

---

[38] Len's point was that air systems on a cost per pound basis are much more expensive than land or sea systems—true, but not really relevant.

[39] I was "in the room where it happened" when John Deutch, then USD(Acquisition) made the decision in 1993 to continue F-22 and F-18E/F, stop the Navy's A-12 follow-on, and start the Joint Advanced Strike Technology (JAST) program that became F-35.

Currently, the Air Force and Navy are struggling to define the next generation of air dominance systems they will acquire for the short-range air domain. Both seem headed toward some form of manned (or optionally manned) tactical fighter or fighter bomber that is an extension of current designs and incorporates more advanced technology, including technology from the Air Dominance Initiative and the Aerospace Innovation Initiatives that I originated and sponsored.[40] Requirements are not final yet, but both seem to emphasize designs that will maximize range and payload and multi-role missions. In addition, the Air Force, and to a lesser extent the Navy, are emphasizing integrating all of their assets into a military internet of things (IOT) in which a "cloud" architecture provides highly coordinated, data analytics and optimized C2 to the force in real time. The AF version of this is called Advanced Battle Management System or ABMS. The Navy version is called Project Overmatch, and the Joint version is called Combined Joint All Domain Command and Control or C-JADC2. Unmanned systems are envisioned as components of Next Generation Air Dominance in both Air Force and Navy concepts, but the mix and allocation of roles between manned and unmanned systems isn't clearly defined, at least publicly and there are many unanswered questions about what the full concepts will entail. Both Services seem open to augmenting manned aircraft with unmanned systems, but not to go beyond that point. Other countries are exploring "loyal wingman" concepts with unmanned systems operating alongside of, or in advance of, more traditional manned tactical aircraft. These efforts are all well intentioned and generally in the right direction, but I believe we need to address some fundamentals that are not being adequately considered now.

First, in the short-range air domain, the dependency on a small number of fixed and very targetable forward bases for conventional take-off tactical range aircraft (a few hundred miles) is untenable. This is true whether the aircraft are manned or unmanned. Fixed land airbases and aircraft carriers operating close to an opponent's coast or border are not survivable enough against current and future threats. This is a development that has been coming for a long time; it was a major concern even during the Cold War—even before the advent of long-range precision conventional ballistic and cruise missiles to say nothing of hypersonic weapons.

Second, the unit cost of modern tactical aircraft, for both long- and short-range air domain applications, their long production lead times, and their expected attrition rate against peer competitors are prohibitive of the ability to afford a force that can conduct a long air campaign. In a protracted peer competitor conflict, the U.S. is likely to run out of airframes if it attempts to conduct operations over a period of months. The F-35 is a good example. I'm a big fan of the F-35; it's a tremendous machine and a major step forward over its predecessors, but only if it can achieve high net cost exchange ratios with very low loss rates against the threats it will face for the next few decades. That means limiting losses on the ground as well as in the air. If it can be based in a survivable way, the F-35 (with adequate investments in continuous upgrades, EW, C3,

[40] The former was a roughly two-year study that I tasked DARPA to lead in about 2012. The latter is a classified technology program that I initiated in 2015 to develop next generation technology in an X-plane demonstration program led by DARPA but with Air Force and Navy co-funding.

air-to-air weapons, and coupled with attritable UAVs) will serve the US well for a long time.[41] Unfortunately, its high cost (including sustainment cost), long acquisition lead times, and basing limitations (except for the STOVL USMC F-35B model) will limit its potential to support a protracted conflict.

If these were the only challenges the U.S. already faces, it would be enough, but there is more. China in particular has been working to develop capabilities that challenge the U.S. directly in the air. This includes attempts to achieve stealth, improved fire control sensors on tactical aircraft (optical and RF), and especially superior air-to-air missiles of various types and ranges that exceed the performance of current U.S. weapons. This last category includes missiles intended to attack standoff counter-air and strike support sensor and C3 systems like AWACS and JSTARS.

We don't have time to waste as we sort out the right concepts for the next generation short- and long-range air domain solutions, but it is also essential we make the right decisions about the future of the air domains. The future concepts I'll describe below can be thought of as the "force after next." The choices the U.S. makes in the near future won't go as far as the concepts I'll describe, but they can take us part way there and make the path to that future shorter and easier.[42] Conversely, if we make poor decisions, we will not shorten this path but increase its length and difficulty. The provocative conclusion I've come to here is both manned aircraft in general, and more specifically the manned "fighter plane" as we've understood it since WW I will become obsolete. Neither the combination of speed and maneuverability as a design driver, nor the emphasis on relatively close-in duels between manned aircraft appears in the concepts I'll describe. Missile maneuverability and speed already dramatically exceed what a human is capable of, and future missile "launchers" or carriers can have similar characteristics—if they are not manned. Tactically required decision times, especially in engagements involving more than a very small number of opposing aircraft, will ellipse anything a human can ever accomplish. "Alone and unafraid" will not characterize aerial combat in the future. The systems carrying weapons (launchers) and the weapons (projectiles) themselves will not be alone, and human capacity, even the absence of fear, will be an impediment, not an advantage.

Operational Concepts

In the short-range air domain, I see no alternative but to avoid the dependency on Conventional Take Off and Landing (CTOL) fixed basing within range of enemy ground launched precision missiles. Hardening, deception, rapid runway repair, and defenses (soft and hard kill), if we were willing to buy them at scale, can all improve the situation, but precision missiles will continue to make it highly problematic to operate from a small number of fixed and therefore easily targetable forward bases. Aircraft carriers can at least move back, and one can talk about using their mobility

[41] Currently the F-35 can amplify the value of existing 4th generation aircraft by working with those aircraft in teams. As tactical unmanned systems are fielded, the F-35 can be used in conjunction with those systems to achieve even higher cost effectiveness.

[42] Force after next, because neither the technology nor the culture is ready to support the degree of unmanned performance that I'll describe.

to do tactical "raids," but sustained carrier operations within range of shore-based missiles are equally problematic. The obvious alternative is the one the USMC has adopted: short take off, vertical landing (STOVL) concepts like the Harrier and F-35B. This is a current option, not a future of warfare potential, but it does point us in the direction of flexible, proliferated, and concealable basing for the forward air domain assets.[43] If we accept this, what should the missions be for a future tactical short-range air domain force and how might they be accomplished? Classically we would talk about missions like offensive and defensive counter air, strike, interdiction, and close air support, as well as a number of supporting functions or tasks like ISR, EW, the suppression of enemy air defenses (SEAD), operational level or above air defense, and airspace management. What I would propose for the future is off-loading as much of these tasks as possible to other domains, especially space, and focusing the forward-based assets in the concept on efficiently delivering weapons against air and surface targets of interest, while achieving enough resilience that attrition levels are acceptable. Integration and optimization using AI tools would also be part of a future concept, but focused on enabling sound automated decisions at the operational edge at the tactical level and supporting higher level operational decisions and decisions for the force as a whole where human interaction is more viable—and valuable.

What I envision here is a clean sheet of paper force design, not dissimilar to the one described for the ground domain in some ways. A future tactical air dominance organization with the missions of providing offensive and defensive counter air and strike (including interdiction and support to ground operations and units), would consist primarily of a group of unmanned stealthy STOVL tactical aircraft serving as weapons launchers. These reusable UAVs would have the core function to operate collaboratively and autonomously in small formations of nominally squadron size (tailored to the operational mission) to deliver weapons against aim points or targets designated by off board sensors. Targets directly relevant to the air domain would include enemy airbases, aircraft, and air defense units. This force would also deliver munitions against ground or sea surface and subsurface targets of interest in support of operations in other domains. ISR, including targeting for both air and ground targets would come primarily from a combination of space, stand-off air, and some ground-based sensors, but as much as possible from sensors and C3 located in space. Stand-off or penetrating unmanned aircraft would provide ISR information as well. Efficiency in the concept comes from relatively inexpensive multi-role unmanned weapons carrier aircraft (launchers) that can operate with acceptable attrition rates, and from the ability of space-based assets to provide wide area threat coverage and timely targeting quality information. Survivable C2 at various echelons would provide optimized weapon target pairing and tactical cooperation among sensors, UAVs (launchers) and weapons (projectiles). Some UAVs could also be employed as decoys and threat weapon "magnets" to draw enemy engagements, thus forcing exposure, reducing threat weapon loads and forcing premature operational and tactical

[43] The Air Force has concepts for alternative contingency basing, but to my knowledge they have not been seriously implemented at scale.

commitment of threat assets. In addition to weapons, the STOVL tactical UAVs could carry decoys and/or countermeasures including anti-radiation missiles and EW modules.[44]

For air-to-air missions, the short-range domain concepts' greatest cost effectiveness challenge is probably fire control sensors and the allocation of functionality between missile seekers and those sensors. The hand-off between fire control sensors and beyond visual range air-to-air missiles is a critical parameter for modern air-to-air engagements.[45] This function is currently performed by highly sophisticated tactical radar platforms like the F-35 and advanced missile seekers on systems like AMRAAM. Optical sensors are taking on an increasing role in fire control as well. While space-based sensors or long stand-off airborne sensors may be able to provide aircraft detection and tracking information, I'm skeptical of their ability to provide the precision fire control information needed to bring missile seekers within acquisition range of their targets. Detailed design trades will be needed to determine the optimal allocation of this functionality—for any future concept.

Once the need to try to keep every platform and pilot safe as much as possible is out of the equation, a whole new range of tactical options open up. Heavy reliance on off-board sensors allows operation from greater stand-off range for air-to-air weapons. Of course, adding range will raise the cost of those weapons. For the air-to-air problem in this domain, some sensing and countermeasure capability will probably be needed on the tactical weapons launcher UAVs. Passive sensors, working in bi-static and multi-static modes would be attractive options to consider from a cost perspective. At this point, I would particularly try to solve the close-in air domain ground attack problem without relying heavily on target acquisition sensors located on the weapons delivery tactical UAV "launchers." This might become necessary, but it significantly increases cost and means those platforms, or a subset of them, have to operate close enough to acquire targeting quality threat data on ground targets from operational altitudes, a few tens of thousands of feet and with limited stand-off ranges, implying much more challenging survivability features. This is the route to an unmanned progeny of the F-35—a penetrating multi-role aircraft capable of operating independently. If it is possible to rely on off-board space-based ISR plus a small number of penetrating survivable dedicated ISR platforms, this would be the preferable course of action. There is a whole new world ripe for exploration here, but the possibilities are quite different from current concepts.

Humans would be involved in C2, preferably at the equivalent of "wing" but possibly, and I think more likely, at "squadron" level, the numbers would be small but multiple "shifts" would be

[44] Concepts like this could certainly be considered. A key to cost effective concepts is deciding what part of the concept is reusable and what part is expended in use. It's the multi-sortie capacity and resilience against attrition that justify the high cost of current tactical aircraft. That consideration would be important in assessing nested concepts.

[45] Air-to-air engagements between fighters in modern times are controlled by the ability of the nose mounted radars or optical sensors on fighters to keep an adversary in the field of view of the sensor and provide fire control quality tracks and guidance information to an air-to-air missile until the missile seeker can acquire the target and proceed independently. In a one-on-one engagement, each combatant is also trying to avoid providing the adversary with the same opportunity. As the number of aircraft in the engagement increases, and the opportunity for collaboration is introduced things get complicated quickly.

required to support continuous operations. These C2BM cells would be high value targets to an adversary, so concealment of their locations would be of great importance. For the short-range air domain concept, I would expect these C2 cells to be ground-based, but limitations on communications networks might dictate airborne battle managers. For the long-range concept, they might have to be airborne, but at as much stand-off range as possible. For resiliency it would be wise to have both options available in each case. The job of C2 cells is to exercise executive control over operations at the echelon level where it becomes both necessary, due to the limitations of communications networks, data integration, and force management algorithms, and practical at the level of control where the speed needed for decision making is relaxed enough that inserting humans is an acceptable time burden. The force concept would also include rapid refueling and rearming—also highly automated—to maximize sortie generation. Human fatigue should not be a factor that constrains operations.

For the shorter-range fight, forward air and missile defenses would be mobile and designed to support preferential defense of regional assets, both military assets and other high value assets. Space-based and stand-off airborne sensors would provide targeting and tracking data to support launch on warning or launch on remote depending on the threat. Operationally, air and missile defense "systems" would dynamically integrate subsets of sensors and launchers to optimally respond to an attack in real time. Ground-based launchers and sensors would be operationally mobile on short cycle times to enhance survivability. Directed energy is a possibility, but weather, threat hardening and other factors make this questionable any time soon. Hardening and deception would be used extensively as would soft-kill (jamming and cyber) countermeasures for defense. I would envision at least a two-layer ground-based air defense arrangement with a higher altitude regional or area defense coverage plus a terminal defense layer. C3BM and airspace management would be fully integrated, and deconfliction between friendly air and ground-based air defense would be significantly enhanced over current practice due to the elimination of concerns about human losses through fratricide. In my view all air domain operations (offensive and defensive counter-air and air defense) should be controlled by a single command using a single highly automated C3BM system.

Both the short-range air dominance and the air defense concepts described should be subject to a host of design trades attempting to get the optimal mix and distribution of features across the elements of the force. These trades have to include every design variable, but they will be driven primarily by cost and anticipated exchange ratios and other factors described earlier that determine operational effectiveness. Modeling and automating the "many on many" air engagement operational situation is particularly challenging, but significant progress has already been made in addressing this problem.

Let's turn to the longer-range air domain situation in which 1,000 miles or more of stand-off is assumed. This is a domain subset, if you will, that most countries will never worry about, but for the U.S., it is critically important. This is sometimes referred to as the "Global Strike" operational environment. An operational force here would have to consist of long-range (multiple 1,000s of miles) weapons carriers or launchers, and standoff weapons with ranges of nominally several hundred miles or more. Alternatively, penetrating weapons carriers/launchers could be used with

shorter range weapons. Defensively, it spans defenses against long-range cruise and ballistic missiles, including hypersonic weapons and penetrating or standoff aircraft as threats. For the offensive mission, the U.S. has relied heavily on penetrating bombers ever since WW II. These bombers carry either gravity bombs or relatively short-range weapons. An exception is ALCM equipped B-52s. Early versions of penetrating bombers used in WW II were not as survivable as their advocates believed, and attrition rates were high, but at the time sustainable, at least by the U.S.[46] Through various measures, the U.S. addressed that problem, notably with low altitude supersonic flight or stealth. The U.S. has kept this penetrating concept central in the B-1 and B-2 designs. Presumably the B-21 is also following the path of penetrating (and therefore expensive) but highly survivable (and therefore reusable over many missions) aircraft, carrying short-range (and therefore cheaper) weapons. Current investments in hypersonic weapons and longer stand-off suggests a change in emphasis is underway for Global Strike offensive operations, but I'm not persuaded this is the most cost-effective approach to long-range counter-air or strike.

There are two sides to the Global Strike long-range air domain equation: offensive and defensive. Currently the U.S. only emphasizes the offensive component. This wasn't always the case. Once upon a time, the U.S. fielded significant quantities of supersonic interceptors for defense of the continental U.S. They were designed to interdict intercontinental-range Soviet bombers well off our borders. We also fielded an operational U.S. continental ground-based air defense system with air defense batteries protecting a number of major U.S. cities (interestingly with nuclear armed missiles). I'm not suggesting we go back to those concepts from the '50s, but in the world in which space surveillance and long-range conventional weapons (including hypersonic boost glide vehicles and cruise missiles) are possessed by our potential great power adversaries, we need to rethink this whole equation, from both defensive and offensive perspectives. As China and Russia continue to acquire long-range conventional weapons, including hypersonic weapons, it's useful to think about the military target sets in the U.S. these countries might find attractive. On that list would be aircraft carriers and submarines in U.S. ports, bomber bases in the U.S., and perhaps critical command and control nodes and some key infrastructure, such as critical industry or the handful of sites that support our information and transportation networks. Ambiguity about the conventional versus nuclear nature of inbound missiles and the risk of nuclear retaliation may be a powerful deterrent to strikes on these targets, either preemptively or after a conflict has been initiated, but I'm not sure we should count on that completely.

The system level design trades for an offensive Global Strike operational concept are driven by the trade-offs in range, cost and payload for the weapons carrier or, in our parlance, launcher. Today, the medium range B-21 bomber is being acquired because Secretary Gates canceled its predecessor, an intercontinental bomber, for excessive cost. Secretary Gates commissioned a "family of systems" review led by Ash Carter when he was USD(AT&L) in the Pentagon.

[46] An interesting and recent, but somewhat criticized book by Malcom Gladwell, *The Bomber Mafia*, describes this era and the debates behind the American approach to the long-range air domain of the time.

Acceptable cost was as much or more of a driver than any operational consideration or requirement, so an intercontinental follow-on to the B-2 was never seriously considered.[47]

A long-range operational strike capability for the U.S. must have a reach of several thousand miles. It must have adequate force capacity overall to be operationally relevant, which means the ability to deliver enough weapons to matter in a reasonable scenario. The reach is the sum of the reusable weapon launcher operational range (including as extended by aerial refueling) and the weapon range—the launcher presumably doing a two-way trip and the weapon a one-way trip. Intercontinental range cruise missiles are conceivable and intercontinental missiles exist, but for conventional warfare both are almost certainly cost prohibitive. Use of tankers and aerial refueling is part of the equation and may be more cost effective than building longer range weapons carriers/launchers, especially if the tankers are already being purchased for other reasons. For the U.S., we now have to decide how important it is to us to attack targets deep inside Russia or China, or to confine ourselves to attacking targets near the coasts or borders. If we are talking about the interior of Russia or China, the weapons/projectiles themselves have to be long-range also (well over 1,000 miles) or the delivery platforms need the capability to penetrate air defenses and operate in the interior of those countries. If deep penetration isn't operationally viable or required, then this weapon range requirement can be relaxed, and the design of the launcher is significantly less stressing—think an arsenal plane cruise missile carrier (like a B-52 or a commercial derivative) versus a penetrating bomber (like the B-2 or B-21). I'm persuadable on this point, but the idea of acquiring a force to execute a prolonged conventional weapon-based air campaign into the deep interior of China or Russia seems prohibitively expensive to me, at least as a peacetime investment. The stressing military operational need for conventional global strike is realistically more likely to be driven by the need to operationally defeat some form of military aggression conducted on the border of China or Russia. If the US retains all three legs of the nuclear triad (the most likely outcome), then some penetrating conventional strike capability will exist in any event through dual use systems. This inclines me toward a conventional global strike concept built around a non-penetrating standoff weapons launcher, carrying weapons with adequate range to be released outside threat land-based air defenses and weapons with the ability to penetrate to operationally important targets, nominally projectiles with several hundred miles in range from the launcher. That takes care of the problem of getting weapons to targets, but this is just part of a global strike concept. We have to address ISR for target acquisition, the weapons mix, details of the launcher aircraft, and C3BM.

To complete the concept, space-based ISR again plays an important role. The problem here is primarily ground or surface targets, a much more tractable problem then air borne threats from a fire control perspective at least. Penetrating survivable airborne ISR would provide redundancy and resilience. Because of the timelines involved for using stand-off weapons against mobile surface targets, there must be updates during the operations while both weapon carriers (launchers) and weapons (projectiles) are in flight. There are cost effectiveness trades to be conducted to

[47] A few years later, when I was USD(AT&L) and about to make the milestone decision to put the B-21 into design for production, I asked Bob Work, who was Deputy Secretary, if he wanted to reconsider whether or not an intercontinental range bomber was a better alternative. Bob chose not to revisit the requirement.

optimize both weapons/projectiles and planes/launchers and a wide range of possibilities that require quantitative analysis. Hypersonic weapons may be cost effective for some targets. Autonomous target acquisition by sensors on weapons or on dedicated loitering expendables may also be of high value. Stealth, defensive aid suites and countermeasures are part of this trade study as well. To protect the long-range launcher platforms, even with significant stand-off, some defensive counter-air functionality would be desirable. My crystal ball isn't adequate enough for me to hazard a guess as to how the details of a full concept study would come out. Such a study should take into account the scenarios and target sets of interest and likely adversarial responses; the details matter, and a mix of capabilities would be needed in a force designed to conduct continuous strike operations over a period of time against a capable adversary.

Building Blocks

In both short- and long-range cases, the design trades for weapons and aircraft should be conducted without the usual constraint of imposing past design specifications of one element of the concept on others. The U.S. has generally either designed new platforms to accommodate old weapons or new weapons to be carried on old platforms. Given responsive and capable threats, new designs should not be overly constrained by legacy designs and growth should be built in so upgrades to higher performance are accessible.

For the short-range concept, the STOVL/VTOL UAVs are attritable and not full-up fighters. They would be subsonic in all likelihood to reduce cost, and maneuverability would not be emphasized. Their mission is to survive well enough to bring weapons—stand-off air-to-air and air-to-ground missiles primarily—into the fight efficiently. They would have sensors and engagement planning only to the level needed to augment the space-based and stand-off airborne ISR and C2 capabilities in the concept. They would be able to act cooperatively autonomously in small groups (like the land concept components) to maximize exchange ratios. The combination of low cost, simplicity, stealth, range, magazine capacity, modular weapons capacity and reuse would be the subject of design trades, but the overall intent is to keep the cost low and to put in just enough survivability to get to missile launch ranges for both air-to-air and strike. Each UAV would carry on the order of six weapons (in some combination of air-to-air and strike) internally.[48] The missile designs would vary based on the target and the sophistication of the threat, but they would have to be designed to overcome terminal defenses, EW, directed energy countermeasures, decoys, and threat maneuvers. Weapons with loitering and independent autonomous targeting for high value ground targets would be included. Small groups of both UAVs and weapons in the concept would be able to autonomously collaborate on tactics against known and expected threats.

For the long-range global strike concept, the stand-off "launcher" would likely be an intercontinental range aircraft with the capacity to carry on the order of 20 or more total internal and externally stored stand-off weapons. The strike missiles would have adequate range to provide at least several hundred miles standoff and they would have the ability to work together tactically

[48] Past studies have indicated that this number is roughly the optimum for air-to-air applications—less is insufficient and more doesn't add much utility.

to maximize overall attack effectiveness. Hypersonic capability might be part of the weapons mix, but I'm not convinced at this point it would be cost effective. Concepts with sub-munitions, various levels of lethality, and variants with features designed to defeat certain target sets would be needed. For defensive air-to-air engagements passive and perhaps bi-static receiver functionality for on board targeting and collaborative engagement using off-board sensors and C2 could be included if cost effective.

In the long-range concept, the "launchers" are basically buses or trucks delivering weapons to a launch point. They need to be reusable to be cost effective and therefore survivable, but with enough stand-off, survivability features can be limited. The planes I envision are not small, as there is efficiency in carrying larger payloads. Given that, similar to capital ships previously discussed, there is no major cost payoff to keeping humans out of the long-range strike aircraft because the delta in weight and cost for having them aboard isn't excessive. (Adding a human to an unmanned aircraft invokes a penalty of about 1,000 lbs.) On the other hand, there may be no major benefit to having human crews in all of the long-range air domain launcher aircraft. Without human crews, as in other domains, tactics that intentionally sacrifice some systems for an operational advantage are more acceptable and can be considered. An alternative is to have a more survivable penetrating weapons carrier or launcher. This would allow for shorter range and therefore lower cost, mass, and volume munitions. If the force's role is to defeat China or Russia's power projection or aggression where the target set is the attacking force, I think the non-penetrating stand-off weapon launcher is the cost-effective approach. If the force is intended to conduct a long-range air campaign deep within China or Russia, the answer would be different.

In both long-range and close-range air domain operational concepts, ISR and targeting quality information could come primarily from a network of space-based sensors in survivable and reconstitutable architectures. This sensor systems and associated C3 systems would be used to acquire targeting quality information to support Global Strike as well as close range operations—against both airborne and surface targets—and to support defensive measures. A fall back or adjunct to those capabilities and a source of redundancy (always operationally attractive) would be survivable unmanned penetrating ISR aircraft. These systems would support real time targeting and retargeting for close-in and stand-off weapons and launchers. For counter-air operations in particular, fire control sensors would probably be needed on the launcher platforms, but perhaps not required on every launch platform.

As noted above, the dominant sensors for decades have been nose-mounted fire control radars on tactical fighters. More recently, passive optical sensors, Infrared Search and Track (IRST) systems, have become important as a counter to radar stealth as their resolution and accuracy have improved. In addition to fire control radars and IRST sensors on tactical aircraft, the sensors that provide the seekers (again optical and RF) on air-to-air and air-to-ground missiles have enabled long-range beyond line-of-sight engagements and the potential for an engagement from one platform to be controlled from another. Finally, off-board wide-area sensors on stand-off platforms

like AWACS and JSTARS,[49] and now potentially space-based, can provide target detection, tracking, and fire control support. The sensor and C3BM architecture in both the long- and short-range concepts is equally or more important than the platforms and weapons designs. The various sensors are all interconnected and interrelated, and their characteristics should be traded off with other elements of the concepts. Just to add even more complexity, the sensor trade-offs are also influenced by electronic warfare provisions, signature management, and the potential for countermeasures of other types.

Turning to ground elements of the air domain picture, the air and missile defense systems for the short-range concepts would provide preferential defense, be highly mobile, employ deception and countermeasures, and utilize off-board ISR and fire control in conjunction with organic capabilities. A multi-layered, or at least multiple shot (shoot-look-shoot) architecture would be highly desirable.

Air and missile defense capability to defend against an opponent's global strike capability would require space-based ISR and fire control sensors and long-range ground-based interceptor missiles. This is a tough mission to make cost effective because of the geometry involved and the options the offense has to avoid to defeat air and missile defense systems, but some capability could add uncertainty, provide a level of threat attrition, and enhance deterrence. Currently, potential adversaries have a limited long-range bombing capacity and no long-range conventional intercontinental missile threat (hypersonic, cruise, or ballistic). But that is likely to change given ongoing adversary research and development programs and the existence of tempting high value conventional warfighting targets in the U.S.[50]

Complexities

Fundamental Operational Needs

Command, Control, Communications, and Battle Management (C3BM): Both the short- and long-range air domain concepts require secure C3BM that supports human-involved operational level planning and largely autonomous tactical execution. In both short- and long-range air domain cases, tactical decisions are made forward and automated. The C3BM architecture must support human decisions, made with AI support and augmenting automation, for a group of assets to be tasked to conduct an operation focused on a set of targets or potential targets in an operational

[49] These large sensor programs on commercial aircraft are very high value targets. During the cold war we calculated that the Soviets would expend 50 to 100 fighters trying to reach and destroy each of these aircraft. Their importance to the outcome of the fight in Europe, both on the ground and in the air, was significant enough that the Soviets would have willingly accepted this exchange ratio.

[50] A surprise conventional strike against CONUS-based power projection systems such our aircraft carriers in port, our long-range bombers on the ground, and possibly key logistics systems such as underway replenishment ships in port or key military port facilities or transport aircraft and tankers on the ground could have a decisive impact on the US' ability to respond to aggression. Arguing against this type of attack is the risk of initiating a nuclear war if the attack is perceived as being nuclear. We have no experience with the escalation risks inherent in a large-scale conventional war between nuclear powers.

block of air, sea, or ground space in a window of time. Once those assets are committed, the group of assets is largely on its own conducting the operation. Humans would monitor the operation (presumably one of many) and could intervene with fairly low latency if necessary. Data flow and processing are kept "forward" at the "edge" as much as possible to limit demands on the C3BM system. Space assets and possibly airborne relay nodes play critical roles in the architecture as do directional and secure communications links.

Logistical Support: The short-range air domain concept requires distributed logistics nodes for rearming and refueling. The logistics infrastructure itself has to be distributed and designed with a combination of hardening, dispersion, and deception to avoid destruction. It must include transportation to support the distributed operational concept. Unmanned systems for ground transport, prepositioned supplies, and resilience are all elements of the concept. The UAV designs should have low maintenance overhead as a result of designs for high reliability, modularity, and for ease of subsystem and component exchange. Humans will be part of the maintenance and logistic support system for the foreseeable future. Many logistics functions and a range of possible complications in support operations in general will require human beings, but their role can be minimized. For the long-range air domain concept, the threat of attack on air bases and the logistics enterprise is less, but not eliminated. Terminal air and missile defenses may be more viable, at least against some threats, but can still be overwhelmed. As a result, logistics operations for global strike missions should be conducted from as many fixed runway options as possible, using commercial airfields and in some cases highways. The options here are finite and prepositioned fuel, munitions, and spares should be covertly allocated to wartime use points prior to hostilities. The planning system should include a "shell game" for returning aircraft to be supported at bases other than the one they departed from.[51]

Multi-Domain Considerations: The air domain concepts provide effects and support into the other domains. When cost, time, distance, reusability of the transport vehicle or launcher, and area coverage flexibility of launchers and projectiles collectively are taken into account, air delivery overall is a very cost effective way to get munitions to operational level sets of targets.[52] As a result the air domain assets will be conducting operations against targets in all the other terrestrial domains—land, sea surface, and sea subsurface. This fact makes control of the air domain essential to victory in other domains. Because of expanded line of sight area coverage, airborne nodes also provide the first or second most cost-effective option for wide area communications and surveillance, with the space domain as its competitor for first place. The air domain therefore plays a critical role in ensuring C3BM and ISR capabilities for all domains are resilient. Airborne assets can also play key roles in EW and cyber for the same reason. Finally, air transport provides the quickest and most responsive, but not the most efficient or necessarily cost effective, way to transport assets for use in other domains. These considerations are enduring and will drive the need for aircraft for a variety of military purposes. Increasingly those aircraft will be autonomous,

[51] I'm envisioning a future in which our adversaries field their own global strike capability, probably with greater emphasis on long-range land and sea-based missiles—there is no fundamental impediment to this that I can see, and they are already fielding systems for intermediate ranges.

[52] For shorter tactical ranges on land (a few tens of miles say), ground-based artillery is most cost effective.

however. The air domain concepts have dependencies on space for PNT, ISR, and secure communications for C3BM. While some of these dependencies can be mitigated through redundant air domain functionality, space (if available) is a much more efficient home for these capabilities.

Resilient Basing and Ground Operations: If an air base isn't survivable and can't be kept in operation well enough to sustain continuing flight operations, it isn't of much use, and the aircraft at the base may be destroyed on the ground or effectively neutralized by being stranded. Operating tactical aircraft is a high overhead enterprise. It involves fueling and arming, maintenance, and battle damage repair. Currently it involves support functions for the humans involved in all these tasks. Each of these activities has a physical footprint as do command and control functions and flight operations functions. Almost any of the items on these lists can be a single point of failure for continuing operations. Protecting a targetable infrastructure against large raids of precision and smart munitions is problematic to say the least. Against smart peer competitors, the only hope is a full array of defensive measures. That would include hardening, deception, rapid runway repair, redundancy, and both soft-kill and kinetic air and missile defenses. I don't believe this can be accomplished well enough to sustain operations at our current known fixed forward bases in Asia or Europe. It is absolutely clear to me our potential adversaries are acquiring the capabilities they need to neutralize these bases with high confidence at the outset of any hostilities. For reasons stated earlier, I do not believe the U.S. can abandon tactical range air domain operations. We have to find an alternative to vulnerable, easily targetable forward basing.

Tactical Mission Variations (Offensive and Defensive Counter-Air, Strike, CAS, SEAD, Interdiction): Both the short- and long-range concepts can perform the range of tactical air missions, with some limitations. Future offensive and defensive counter-air engagements should be dominated by beyond line of sight engagements. The counter-air engagement equation is about seeing and shooting first and having enough of an advantage in reach, missile time of flight, maneuverability, acceleration, and stealth that an air-to-air missile launching aircraft doesn't suffer mutual destruction with the engaged target from a similar enemy missile fired before the enemy aircraft's defeat. Part of the idea for the short-range concept above is to make the aircraft's cost low enough that even a one-to-one exchange ratio is still favorable on a cost basis, but the concept doesn't depend on that. If off-board targeting of air threats can be accomplished from survivable assets in space, or from stand-off airborne sensor platforms, then air-to-air missiles can be launched at maximum engagement ranges. The potential for multi-UAV collaboration in the many-on-many or few-on-few air combat situations also provide the opportunity for aggressive tactics that accept some losses in return for overall advantage. For example, if the short-range concept is operationally responding to a large-scale attack, it should have a target rich environment, and an individual UAV can be exposed with the expectations it will be able to launch successful attacks on multiple targets based on off-board fire control before being destroyed. This cycle can then be repeated. In the long-range concept, if enemy defensive counter-air was a viable threat, similar tactics could be employed, possibly with even longer-range stand-off air-to-air missiles. Strike operations in general would be enabled by off-board targeting and autonomous seekers on stand-off weapons which would enable autonomous ground or sea surface engagements. Both concepts

could provide strikes in support of forces in contact or forces within a few tens of miles of contact (CAS and interdiction as I'm defining them) based on off-board targeting and or ISR adequate to release weapons with autonomous seekers and appropriate automated rules of engagement.

Target Identification, Deconfliction, and Collateral Damage Avoidance: For the types of scenarios of greatest concern, the operational context would provide strong or even conclusive indicators of target identification. In other situations, more stringent control measures can be enabled and, in some cases, remote human-in-the-loop control if it is necessary. In both concepts inflight updates and changes in rules of engagement should be provided, for both weapons and aircraft. Deconfliction is important to cost effectiveness. For many-on-many or few-on-few situations, collaboration to avoid conflicts and to maximize the effectiveness of the attack is an important part of the concept and has to be designed in (an analogy is all the kids on the field running to the soccer ball).

Design Requirements and Considerations

Air Base Survivability: Even for the long- and short-range concepts above, air base survivability will still be an important consideration. The more remote range for the long-range concept does not protect bases from long-range cruise, ballistic and hypersonic missiles. The short-range flexible and agile basing for the STOVL aircraft in the concept helps but isn't a panacea. The U.S. has long neglected active defense, hardening and deception/concealment in favor of acquiring larger force structures. I won't dig into why this is true here, but given the threats we have to prepare for, that needs to change.

Airspace Management and Control: This is a broad area that encompasses operational planning, dynamic replanning, deconfliction (not just among aircraft, but also for ground fires of rockets and artillery, and any directed energy radiation), identification friend or foe (IFF), and collision avoidance. This is essentially what the ABMS and JADC2 programs are trying to enable now. Unfortunately, the U.S. has had several false starts in this area, (SIAP, AOC upgrades for C3BM and 3DELRR for ground-based radar, for examples) and is at risk of repeating this history. I don't see a technological showstopper to creating a highly integrated, flexible, and responsive system that incorporates some AI technologies and a modern communications architecture, but the difficulty of achieving this vision shouldn't be underestimated and reasonable steps toward the goal have to be well defined, manageable, and contribute operationally in measurable ways.

Anti-Tamper: Aircraft and the things they carry will come down where enemies will gain access to them. They either must have strong anti-tamper defenses against reverse engineering and exploitation or features we don't mind our enemies having access to.

Battle Damage Repair and Resilient Design: There is a long-standing design discipline for military aircraft survivability and rapid repair of battle damage going back to the early days of air warfare. Fused fragmentation warheads on air-to-air and surface-to-air missiles can partially damage their targets over a wide range of outcomes. Without people in the aircraft, however, a lot of the motivation for damage resilient features intended to increase the probability of successful aircraft recovery disappears. Also, with light footprint flexible basing, the case for battle damage repair

overhead is weakened. Even so, it can be cost effective to include some level of resilience and to provide for some repair of surviving platforms that manage to return to base. This should be a conscious trade-off, not a default to lowest cost.

Confidence in Automated Behaviors: Most safety of flight related behaviors will mature in parallel in the commercial world and can be demonstrated through testing and simulation. Combat-related automated behaviors will be much harder to verify. These behaviors must be operationally effective, preclude fratricide, avoid collateral damage, and minimize redundant engagements. It will also be important to verify the effectiveness of both baseline tactical behaviors and validate evolving tactical behaviors acquired through machine learning.

Countermeasures: Each platform in the concepts may carry a range of active and passive countermeasures (radar and missile warning sensors, electronic warfare systems, decoys, and expendables) based on cost effectiveness and expectations for the expected adversaries. Versions of these countermeasures for current threats already exist in many cases, and more are always in development. Technology is enabling more integrated and responsive systems across platforms as well as collective automated learning from both training and combat experience.

Cyber and EW: Cyber threats must be hardened against to a level that provides confidence the platforms and weapons in the concepts cannot be defeated through cyber means. EW is a continuously evolving area. The most recent innovations include cognitive EW embedded in multi-use radio frequency systems that also act as sensors and communications devices. The EW architecture is an important part of the trade spaces for long- and short-range concepts. It encompasses electronic support measures, self-protection jammers and stand-off jammers. At this point I couldn't say what mix of dedicated escort, stand-off, or self-protection jamming makes sense in either concept, but I would lean toward escort jamming for the short-range concept where a subset of the UAV systems in a formation would have this dedicated role and self-protection jamming for the long-range weapons launcher UAVs in the long-range concept. All platforms and weapons should be designed to reduce vulnerability to EW threats as much as practical (low probability of detection and intercept RF designs and embedded radar EW countermeasure techniques for example).

Deception: The fairly standard ground-based concealment, signature management, and decoy concepts apply here, especially to the forward based short-range concept. The U.S. has spent decades free from the threat of air attack. Our adversaries have long emphasized these areas much more than the U.S. has—this has to change. There is also a good potential for deception operationally in the air where false targets or sacrificial UAV decoys can be employed to precede "real" platforms and draw fire, reducing threat inventory and causing the threat to expose itself. Anything that creates uncertainty and delays or distorts threat reactions should be considered for inclusion in the concept designs.

Default Behaviors—Loss of Contact/Control by Echelon: A wide range of possible situations have to be anticipated, both in principle and specifically, and programmed for. There are the obvious "return to base" situations, but others are more complex. Actions if a primary target is not found, weather implications, default behaviors for loitering weapons are examples. In a many-on-many

highly automated operational context, it is not going to be practical to have humans in a remote location access all the needed information to make judgements about every platform or weapon level tactical decision that becomes necessary hours after a strike formation is launched. More executive level operational decisions, such as abandoning an attack entirely because of the resistance level, or shifting a formation to another operational area entirely, should be made by human decision makers. Overall, I would anticipate the need for some baseline default behaviors and a range of tailorable preset and adjustable options depending on the tactical situation.

Energy: Current energy sources would be acceptable for the concepts described, but as more efficient sources become available, they can be adopted for use. The infrastructure to support refueling at operational tempos would be necessary for both long- and short-range concepts and would have to be resilient to operational threats.

Humans—Location, Role of, and Support To: As in the other future concepts, humans have a critical executive level planning, oversight, and command role. They are also necessary for some support functions which cannot reasonably be automated in the foreseeable future. Humans will also have a role in interactions with other parts of the joint and combined force, and with civilians. These are either operating base functions or performed from a secure mobile C2 facility. I would anticipate the command-and-control staffing for a wing size force nominally to be a few tens of people. Operations would be controlled at either the equivalent of a wing level or possibly at the equivalent of a squadron level. For survivability reasons, I would not collocate C2 elements with actual UAV operational locations. Some support people would have to be at those locations to perform any functions that couldn't be automated.

Identification Friend or Foe (IFF): The IFF systems used commercially and that have military modes will probably still be with us in some form in the future. I anticipate other non-cooperative means would be used to confirm identity and classification to provide better situational awareness and threat assessment. There are a number of signatures (active and passive) that can be merged to provide for both friend and foe identification. The automation of this function is crucial for multi-platform engagements in situations where the environment is relatively target rich and time is a critical variable. Some tactical situations will be fairly unambiguous, if the right data gets to the right place to allow decisions at the tactical edge. Other situations (see pre and post merge item below) will be more problematic.

Interoperability: Interoperability is particularly important in this domain because one of the most important contributions the US can make to its international partners is assistance with control of the air and negation of threatening adversary ground or sea-based forces from the air. The long-range concept should be capable of assisting any ally in any location in operationally useful timelines. To do that successfully, the US needs to obtain and share reliable situational awareness and target identification from and with partners. That information allows U.S. air forces freedom to operate against those targets and it maximizes the effectiveness of allied systems. Interoperable information exchange is also necessary to ensure allies didn't engage U.S. aircraft by mistake. Human presence in allied command centers and experience gained through exercises (virtual and live) are probably equally as important as technical interoperability.

Legal Constraints: The greatest concern here may be limiting collateral damage to unintended (meaning non-combatant) ground, sea, or air targets. Weapons in the concepts are going to be beyond-line-of-sight fire and forget for the most part. In some cases, weapons will be monitoring a ground or sea surface area for hostile targets of opportunity to engage, either independently or in groups. In dense many on many situations, the rules of engagement will have to meet legal constraints while still allowing automated and cost-effective engagements. In other cases, where time and the threat situation permit, there should be provision for humans in the loop to minimize collateral damage.

Mission Planning, Including Dynamic Replanning: Although the lead times for long-range mission packages and short-range mission packages are substantially different, the planning and dynamic replanning functionality is similar. A mission package of launchers with associated weapons, sensors, and supporting functions such as EW, cyber, and deception is created with human executive supervision enabled by automated modeling and simulation. This is a complex task with a lot of moving parts and done with a great deal of uncertainty about enemy actions and responses. As an operation unfolds, and new information becomes available, replanning and re-tasking should occur on short timelines. Realistic data loads and decision timelines will dictate some degree of delegation to lower echelons and greater autonomy as decision time is effectively compressed. At the engagement level in high intensity operations, decisions will be highly automated with human monitoring.

Operational Planning and Rehearsal: Automated tools that simulate mission package interactions will be run continuously to plan operations and to assess likely outcomes and compare courses of action. These tools should learn from operational experience to improve their performance. Threat models should be continuously updated. Currently, air operations involve multiple concurrent planning cycles with different lead times and levels of fidelity. I would expect that paradigm to continue, but with more feedback and "feedforward" between different lead time planning efforts than currently occurs.

Pre and Post Merge Situations: In general, both concepts envision engagements conducted from beyond line of sight. While these pre-merge situations might be preferred (they will be preferred by at least one participant—hopefully the U.S.) post-merge confused situations with intermingled friendly and enemy aircraft will still happen. One side may work hard to force this situation and even accept losses to create it. It's especially hard to avoid this for the short-range concept. Individual and small group collective automated tactics will have to be developed for these situations. DARPA has already made significant progress with this technology.

Physical Security: Against a future peer competitor, there is probably no sanctuary associated with range, but the likelihood of discovery and line-of-sight ground attack, small UAV attack, or short-range indirect fire attack is much higher for the short-range forward operating elements of the force. The security of the logistics, command, and communications functions must be provided for as well—at both short- and long-range concepts. I would expect a combination of humans and autonomous systems would be employed for this purpose, with the bulk of the effort provided by

automated means, but some human presence for dealing with more complex situations and some interactions with other humans.

Responsive Threats: For the short-range concept, the first reaction would be to try to find and target STOVL systems and/or their logistic support on the ground—by any means possible. For ground targets, deception, mobility and hardening would be emphasized against both long- and short-range concepts. In the air, tactics would be developed to try to improve exchange ratios. Longer term I would expect to see similar concepts fielded in response, but with designs intended to outperform those the U.S. had fielded. For example, extended range engagement of long-range stand-off weapons launchers and sensors would be considered high payoff. Space assets used for targeting and communications in support of both concepts would also be even more important for an adversary to threaten—by any means.

Requirements Creep: Conscious attention should be placed on avoiding cost imposing marginal or low return on investment requirements. The natural tendency in all domains is to add more and more requirements to the design until the concept crashes from its own weight. A lot of the items on this list are good examples of potential requirements creep, if taken too far. The whole point of the concept is improved cost exchange ratios over current systems.

Single Points of Failure: The planning chains and kill chains in the concept should be designed so there is no single point of failure and so there is graceful degradation as assets in the concept incrementally experience attrition or are defeated. I'd be especially concerned about the logistics support network for the forward deployed and distributed STOVL aircraft and about the communications links that provide situation awareness and targeting data to planning nodes.

Stealth: For the foreseeable future, stealth will still very much be part of the equation. Operationally comparable optical and RF (full spectrum) stealth for sensor wavelengths of interest is highly desirable and I believe technically feasible (with the exception of aircraft and missile rear aspects), at least until quantum sensing becomes available. For the long-range concept in particular, stealth should also be applied to the stand-off weapons in the concept.

Training, Experimentation, and Testing: Virtual many-on-many simulated operations and engagements are the key to developing advanced tactics and effective integrated mission planning. Operations in the air, with targeting and situation awareness provided from space, are likely to be decisive in a future conflict. The models and simulations that will plan and control these operations have to be based on realistic and extensive training, experimentation, and testing. Combined live, virtual, and constructive experimentation and testing will be the tools to train the artificial intelligence algorithms that would do real operational planning. Nothing will be more important to success. If we can't demonstrate substantially improved exchange ratios and higher battlefield efficiency for air campaigns through experimentation and testing, then we won't achieve them in practice against responsive threats.

Other Needed Military Functions

Airlift—Strategic and Tactical: The history for the U.S. has been to develop and purchase military specific aircraft like C-130, C-5, and C-17 for tactical and strategic airlift. Tankers tend to be commercial derivatives. There will certainly be a need for these functions, but over time they will probably move to unmanned platforms, at least for most of the inventory. Optionally manned may well make sense for these systems into the foreseeable future because, as in other large platforms, the delta cost to provide for human manning is relatively low and it provides flexibility for a wide variety of situations. Given the vulnerabilities of large commercial airports, I see a continuing need for aircraft capable of operating from austere locations. Fleet sizes and aircraft capacities would need to reflect expected operational scenarios.

Close Air Support: An artifact of relying on primarily unmanned systems, especially unmanned lethal small VTOL UAVs, in the tactical ground domain is close air support becomes a less contentious issue. All the emotional aspects of defining close air support and decisions about doing or not doing close air support and how much to invest in it (or not) can be approached more objectively.[53] I spent several years chairing a close air support coordinating group in the Pentagon in the '80s and '90s. It was a struggle to get the Air Force to put resources into the close air support mission, which was seen by the AF as a low payoff use of valuable airplanes and crews that could be attacking much higher priority targets than the enemy ground forces in contact with individual Army units. Of course, Army infantry platoon leaders and company commanders had a different take on what those priorities should be. Without humans at risk on the ground, the relative priorities for determining how to allocate aircraft strike sorties and optimize weapons load outs could be much more objectively determined based on desired operational outcomes and relative cost benefit analysis. The heavy reliance on armed small UAVs in the ground concept also reduces the need for CAS from non-organic air assets.

Combat Rescue: At some point as piloted or crewed fighter and bomber aircraft are eliminated, the need for combat rescue dissipates as well but it probably isn't eliminated entirely. There will still be some need for extraction capacity—for a range of missions and circumstances including some special operations or covert operation situations. There is also a dual use value for humanitarian or noncombatant evacuation purposes. I would expect this capability in the future to be provided by unmanned systems, however. It would allow for higher performance aircraft and more assumption of risk on the ingress portion of a mission particularly.

Disaster Relief and Humanitarian Assistance: Aviation assets, both rotary and fixed wing, play a major role in disaster relief. That mission will still exist, and DOD will be tasked to support it, but it will be a collateral capability and not a major driver for the systems acquired by the DOD. The supply function can be highly automated and conducted with the airlift assets discussed above. Other specialty capabilities, such as medical treatment, medical evacuation, services restoration,

[53] When I was Deputy Director of Defense and Engineering for Tactical Warfare Programs in the early 90s, I chaired the DOD Committee on Close Air Support. It was painful to lead the negotiations among the Services over how much the AF would spend on this mission, if anything.

and anything involving significant interactions with the local population will still involve humans for the foreseeable future.

Interdiction: This is actually a core mission of the envisioned air domain forces, for both the short- and long-range air domains. These future air force concepts are designed to defeat an adversary's power projection efforts. The principal targets are initially offensive enemy air forces (in the air and at their bases), to secure freedom of action in the air and to defeat air attacks on U.S. and friendly forces, and then interdiction against advancing enemy forces (on sea or land) and against ground or sea-based missile launchers that are supporting that advance. Because of the importance of the space domain to operations in all other domains, space related targets (launch systems, space surveillance, and ASAT systems for example) would also be high priority targets.

Medical Evacuation: This capability will be required, and it will still involve human caregivers for the foreseeable future but given the reduced reliance on humans in the various domain concepts, the amount of this capability needed will be significantly reduced.

Mine Warfare: This is debatable, but I don't see the U.S. moving to significant reliance on or utilization of air delivered mines to support land warfare. In addition to the concerns about collateral damage and disposal, there is a cost effectiveness concern about integrating land mines with maneuver and fires. Mine use in sea surface and subsurface maritime domains is more attractive, given the threats and the areas of operation in which sea mines could be employed against potential adversaries. There isn't much in the way of new technology needed to field bottom moored or emplaced air deployable smart maritime mines for use against threat surface ships and submarines. Operational concerns about feasibility of deployment, timing relative to threat actions, endurance, command and control, and net effectiveness should be analyzed before going down this path too aggressively. On the countermine side of the equation, there is a potential role for airborne countermine sensors and delivery of countermine sensors and neutralization payloads for sea mines. Both applications could be accomplished by unmanned air vehicles.

Noncombatant Evacuation Operations (NEO): Airlift plays a heavy role in NEO when time is limited and extraction of civilians at risk is the high priority mission. Commercial air would be used as much as possible, but if conditions dictated military airlift could be used as well. This can be a complex mission with a strong need for human presence to deal with security, government-to-government coordination, and just the complexity and unpredictability associated with a situation where a NEO effort has to be conducted.

Special Operations: Specialized air assets, rotary wing and fixed wing, play a major role in a range of special operations missions. Operations like raids, extraction, insertion, hostage rescue, etc. involve a great deal of both detailed planning and rapid adaptation to changing conditions. The complexity and unpredictable features of many of these missions implies to me there will be a strong human element to conducting these missions for the foreseeable future. UAVs are already used to support these missions, and their use will expand, but they will continue to be tightly human controlled operations and often involve human operators on the ground for the foreseeable future. That said, technology will provide the humans involved with advanced unmanned platforms and automated tools to assist with planning, rehearsal, and execution of these missions.

Strategic Air Campaigns: The forces envisioned could conduct air campaigns against an adversary's economic infrastructure, or other strategic target set using conventional weapons, but neither the long nor short-range concept was designed with that capability in mind. This can be a practical and effective way to coerce a lesser power, as was done against Serbia. However, I don't see a protracted strategic air campaign as a practical reality when dealing with countries like China and Russia, with both large nuclear deterrents and high capacity to absorb damage while extracting losses through attrition. The risks and the costs of sizing a force for this mission seem prohibitive to me.

Suppression of Enemy Air Defense (SEAD): This capability will be required and specialized weapons (kinetic and non-kinetic) and tactics will be needed to execute this mission.

Warfare Domains – Space

Introduction

In the air domain, I described two needed concepts. For the Space Domain, I will discuss two somewhat separable conflicts instead of one; a future offensive conflict, where one tries to eliminate an adversary's space capabilities; and a future defensive conflict, where one tries to defend one's own capabilities against attack. This stems from the nature of space as having military value largely as a location from which to provide support to operations in other domains and from the fact that space systems are generally either one or the other—support systems or weapons—but not both. In a space conflict there are no fixed territories or zones of control to defend and attack; everything is intermingled. Conceptually then, there are two overlapping warfighting missions in space; providing and protecting the support functions we depend upon space for and denying similar support to adversaries. Some tools apply to both conflicts, but many do not. Also, because the carrier, launcher, projectile construct would primarily apply to only the offensive mission and would not in my view simplify the discussion appreciably, I'll forego that awkward intellectual exercise and drop that construct in this section.

Space as a warfighting domain has another unique feature; there has never been a real conflict in space. In other domains, such as sea surface, there may not have been a major peer-on-peer conflict with modern military technology for several decades, leaving us without any relevant current experience to guide us. In space, we have no warfighting experience to guide us at all.

In about 2014, I showed the Deputy Secretary of Defense's senior budget deliberating body, the Deputies Management Action Group (DMAG), a PowerPoint slide I had constructed that characterized the choices in space facing the Department of Defense. As I recall the slide, it depicted alternatives necessitated by the fact that China and Russia were both developing a suite of space control systems designed to kill the satellites the US depended on for intelligence, communications, navigation, timing, missile attack warning, and missile defense. Our most important assets in space numbered in the few tens of satellites and were in predictable and visible orbits. For decades, we had operated those assets with almost complete impunity from attack. That time was fast ending if it had not already. My point was the Department had three choices. We could keep building these kinds of often multi-billion-dollar satellites and try to defend them; we could rethink our space architectures and create more resilient or defendable architectures; or we could reduce our reliance on space-based assets. Business as usual was not a viable choice. I pointed out that peacetime intelligence collection requirements—the traditional mission of the National Reconnaissance Office—argued for very sophisticated high-resolution sensors, and therefore large, complex and expensive satellites that are very hard to defend in a conflict. Our warfighting needs and our peacetime intelligence needs were diverging. We could either reconcile those requirements somehow or build separate systems for the two missions. I've become increasingly convinced we will be forced to do the latter; peacetime intelligence collection systems are needed, but they will go on being small in number, big in size, high in cost, and vulnerable to attack. They can be hardened and defended to a degree, but at the end of the day they will not be able to survive against a determined, capable, and well-resourced adversary.

In about the same period of time, we were also trying to define the content of the "Third Offset Strategy" concept that DSD Bob Work had initiated. As part of that effort and as mentioned earlier, I chartered a Long-Range Research and Development Planning study chaired by Steve Welby, ASD for Research and Engineering. One of the critical questions I asked that group to address was whether we should continue to rely on space for the important military support functions it provided, or shift to other domains and assets, such as stand-off or penetrating long endurance unmanned airborne systems. The group's answer (which I accepted at the time, but which I'm still not 100% sure was correct) was to increase our reliance on space systems rather than decrease it. To do this we had to design space architectures that could survive attack and/or be quickly reconstitutable at reasonable cost. That was the course of action recommended by the study. Several years later, the Department of Defense is moving in that direction, but still has not fully resolved the issues of just what the U.S. space order of battle should be, how much resilience is needed, or how it will be achieved. We now have a Space Force and a Space Development Agency, but we have not answered some fundamental questions: what will war in space look like in the future, and what order of battle should the U.S. invest in to prevail.[54]

In addition to the support functions the United States has come to depend upon, we will also need an offensive space capability. While it is highly desirable to maintain space-based capabilities in a conflict, it is essential to deny them to threat nations. An adversary cannot be permitted to retain access to persistent targeting quality data to support operations. I have a hard time imagining a future great power conflict in which achieving control of space would not be decisive. For a country like the United States, whose military is built around the ability to project power and to defend far forward, being able to decisively deny an adversary observation from space is as essential as control of the air has been to ground and sea operations for the past several decades. For this reason, offensive counter-space systems should be a priority investment for the U.S. As an aside, it may be possible to limit at least some offensive capabilities of a potential adversary through international agreements. I'm skeptical this can be accomplished, but the potentially hair trigger nature of war in space and the perception of a first mover advantage suggests that effort should be undertaken. I'm reminded of the naval arms races that in some part led to WW I and WW II. It would be wise to avoid going down that path, but we have already started, and the pace is accelerating.

Policy people like to talk about space being crowded, congested, and contested. Military operators like to talk about it as a warfighting domain and as the "high ground" in future conflicts. I'm inclined to think of space more as a sort of no-man's land. Both sides have it under continuous observation, both sides can cover it by fire, and there is limited opportunity for concealment. During a conflict, space becomes a hard place to survive, especially over time. Passive systems have a better chance to survive than active systems, but to be useful almost all space systems must be able to receive and send information. In peacetime the no man's land analogy breaks down. In

[54] As an aside, when one creates a Space Force, one can expect that institution to see more spending on space as the solution to any threat to space systems, rightly or wrongly. We've created a new bureaucratic and political power center that will inevitably try to increase its own resource allocation. The need for such a power center was probably the most compelling argument for creating the Space Force.

peacetime space is open to all and there is high opportunity for deception. This fact grants a potential adversary an opportunity to conduct reconnaissance, gather intelligence, covertly or overtly station sensors and weapons on orbit, and prepare the battlefield in detail prior to the start of hostilities. Presumably deception would be used to achieve some objectives surreptitiously. This situation is tactically and strategically unstable; it can make the risks of not moving first to attack the other side appear very high during a period of tension. Think of space as a chess board where both sides get to preposition pieces prior to the start of the game, without full knowledge of the other side. Then either side can start the game at its own discretion by moving all of its pieces at once. The rewards for going first, and the penalties or risks for going second, are very high.

All of this is a new dynamic and one that has not been explored or thought about very well at scale. Most war-games and scenarios I've seen concern themselves with limited scope and short-term attack scenarios—more like sniping or skirmishing than a full out assault. The reality, I'm afraid is an adversary would move quickly and decisively, with surprise, if possible, to completely destroy all relevant adversary space-based capabilities (note that destroying capability is not the same as destroying assets. There is a high payoff to identifying and destroying key nodes, such as unique C2 assets, that can bring down an entire suite of capabilities). Ground stations and launch stations would likely be attacked as well, especially the more assessable overseas assets if there was a desire to avoid "homeland" attacks. The attack would likely blend all available types of attack.

Future space conflicts will be characterized by a high degree of automation and autonomy. Space systems are already going to be unmanned and largely autonomous, especially once they are committed to a course of action. High fidelity war game participation has taught me time is a critical parameter during a conflict in space. Orbital transfer times, ascent times, fuel burn times, and the tyranny of orbital mechanics conspire to limit operational choices very quickly as decision time compresses. In this construct, effective automated decision making for battle management can be a crucial determiner of outcomes. Humans may be able to monitor and override automated battle management tools, but those tools and their ability to successfully simulate many on many engagements and optimize actions will be essential to success—for both defense and offense. There is another destabilizing offense defense asymmetry here—the attack planner may have infinite time to plan and rehearse an attack. If a conflict begins by surprise in space, the attacker can choose the most ideal time for the attack from several perspectives. The defense does not have these advantages; it must respond in real or near real time and do so at a moment the attacker has chosen as the least favorable moment for the defense. Because a successful surprise attack in space can also be decisive for operations in other domains, the temptation to launch such an attack can be very high, especially if it is seen as preempting a similar attack on one's own assets.

Operational Concepts

The operational concept for the offensive side of a future war in space is fairly straightforward—build a mix of various means of attack intended to optimize results and employ them together in mutually reinforcing, redundant, and decisive ways. Build in redundancy so if one attack method

fails another can still be successful. Acquire enough capacity that after an initial exchange, one still has the ability to quickly destroy any attempts at reconstitution. This is not the future of space warfare—it is the present. In this construct a number of considerations affect the mix of weapons. For example, weapons that can be effective instantaneously and simultaneously are preferred. Ground or sea-based kinetic attack mechanisms have the disadvantage of longer flight times and greater difficulty concealing intent. For these surface-launched systems, it only takes a few minutes for LEO attacks and a few hours for GEO orbit attacks. These time frames aren't prohibitive, but any warning time can be used by an adversary to maneuver away from an attack or take other defensive actions. These weapons do provide better opportunities for damage assessment than some other attack modes, but they also can produce significant space debris. In a major power conflict this risk might be acceptable, at least to an adversary. The mere existence of potential adversary direct ascent ASAT inventories today strongly suggests this is the case for Russia and China. I won't attempt to describe an optimal future mix for the United States; it depends on policy choices, operational intent, and threat considerations. There is no real technical constraint on acquiring a desired mix of systems today.

The operational concept for the defensive side of a conflict in space is the asymmetrical dual of the offensive concept. Build an optimized suite of capabilities and use them in close collaboration to preserve and reconstitute the suite of capabilities needed to support terrestrial operations in the other domains. The tools and techniques available to ensure the survivability of space-based capabilities have been discussed publicly, albeit speculatively, for many years. They include hardening (shielding against lasers or microwave devices, for example), avoidance (detect the threat and maneuver away), disaggregation (breaking up capability into smaller units—many of which would have to be attacked to defeat the capability), proliferation (just buying more assets to have multiply redundant capability), concealment, replenishment (war reserve assets that could be launched quickly to give a temporary capability as needed), defense (putting sensors and defensive weapons as well as counter-measures on satellites or near them), counter-offense (attack the anti-satellite systems on the ground before they can be used), and deception (e.g. make military assets look like much more proliferated non-military systems).

A viable space architecture designed for wartime survivability would include most if not all of these elements, but given my comments on the benefits of surprise, there should be a high premium on concealment and deception. An adversary's well planned and coordinated attack will not succeed if he doesn't know assets exist or where they are. Even with this feature, a space support architecture would also have to include a sophisticated operational planning and decision support system that could react in near real time to threat actions as soon as information became available. One of the goals of this concept would be to create high uncertainty of attack success in the mind of an adversary. Fear of failure is a powerful deterrent. In addition to increasing the resiliency of space-based systems against attack, it would also be wise to supplement that capability with fallback ground, sea, and air-based systems that would provide some redundancy and reserve capacity for the most critical military functions currently provided from space: reconnaissance and targeting; communications; position, navigation and timing; and attack warning.

Underpinning both space offense and space defense warfare orders of battle, there would have to be a robust space situational awareness capability with the capacity to monitor all activity in space continuously and with high fidelity. A major problem with US space situational awareness today is the degree to which it was designed for a peacetime environment, without adequate concern for resilience or survivability.

Secure, resilient, and responsive access to space is also required. Today both launch capacity and space systems are acquired on something like a "just in time" management approach. If we are serious about space warfighting and reconstitution, the U.S. will have to acquire a wartime reserve of both launch capacity and satellites. Launch facilities and ground stations will also have to be more survivable and redundant, suggesting either concealed locations or, more likely, mobile systems.[55]

Command and Control and Battle Management for both offensive and defensive space operations will be highly computationally intensive and highly automated; the operator's role once a serious conflict is initiated may be to simply engage a system of automated responses. An AI driven course of action alternative analyzer with scenario analysis capacity well beyond human reasoning or intuitive potential will be needed to create real time responses and direct their execution. Human override will be possible and probably insisted upon by operators. Unlike other domains where tactical decisions can and should be decentralized to the "edge," there will be a need in space operations for more centralized decision making and execution. It's quite possible the space conflict battlespace will be partitioned into GEO, MEO, and LEO "fights" modeled and directed with some degree of independence from each other. Whether this architectural decision is made or not, the number of simultaneous interrelated actions that will have to be taken would still overwhelm human operators, even with fairly sophisticated tools. Once the space war starts, humans will largely be observers of the actual engagements—if our ability to "see" what is happening has survived. Humans will be involved in decisions about options with longer, less stressing time horizons and more strategic impact—such as when to launch a reconstitution effort or when to unleash a second wave of attacks.

One important thing to note at this point is the Space Force concept conjured up by the description above is not a trivial matter and it is far from what we have now. It is also not something that has to wait for new advanced technology to be developed. While the fledgling new Service just created has a very small end strength and a budget a fraction of the other Military Services, getting from where we are today to a force that can sustain its functions against a determined adversary and decisively take on that adversary's own space systems will require a substantial investment, and a major paradigm shift in how we think about space. As this picture comes into focus, the choices I presented to the DMAG several years ago will have to be addressed and a question I've been asking for years will have to be answered. What is our future space order of battle, and how do we get from here to there?

[55] The proliferation of commercial launch systems for smaller payloads may partly address this need.

Building Blocks

At the end of this section, I'll provide a list and some discussion of the specific functional types of systems I think we will need in the future as building blocks. Some are firmer than others, but all should be analyzed and considered. Many exist today but are not designed for conflict in space.

While the functionality of the space-based building blocks is reasonably clear, the optimal combination of mass, orbital planes, individual satellite mission capability, design life, sustainment concept (if any), and combination of defensive features will all have to be the subject of detailed and highly classified technical and operational trade studies. My short answer to how those trades will come out is "I don't know." My experience suggests there are "sweet spots" in the area of a few hundred pounds of mass for most payload applications, but that can change as technology evolves. There will need to be some degree of distributed, disaggregated (not the same thing) constellation designs for survivability, and there will be a premium for concealment and deception in general and in the context of the mega-constellations commercial firms are just starting to build. The NRO concepts of large, expensive, and highly targetable satellites will almost certainly not meet the warfighting needs of the Department of Defense, which will have to acquire its own tactical and operational surveillance and targeting capabilities. There is a good probability any military satellite constellation will not be survivable in space against a determined adversary. If that is the case, reconstitutable space support systems launched in conjunction with an operational need and which are not expected to survive beyond a short operational window will be needed as a building block—together with a survivable mobile launch capability. Beyond that, there is a lot of engineering and operational analysis still to be done. My sense is current design constructs have not taken responsive threats adequately into account. That needs to change before we make major investment commitments.

It should also include the ability to attack relevant enemy terrestrial space related assets with conventional weapons. Directed energy in the form of ground-based lasers in particular should be considered for inclusion, if the technology can be demonstrated to be adequate, which I believe it can be in the future. Soft-kill mechanisms including EW and cyber should be fielded as well, and continuously upgraded.

Here's the mix of systems I think we will need or should at least consider:

Offensive Systems:

> Direct Ascent ASAT: These systems have been fielded already, but not by the U.S. The U.S. did test an air-launched ASAT in the '80s but abandoned the program. More recently, a U.S. Navy Standard Missile was used to intercept a de-orbiting satellite as a safety precaution, but this missile has very limited ASAT capability because of its kinematic characteristics. Russia, China, and others have conducted direct ascent ASAT tests very recently. A ship-based or ground-based system would be more responsive and easier to keep in a high readiness state than an air-launched system. It could also be dual use and affordable in reasonable numbers.

Directed Energy Weapons: Over several decades the technology for ground-based laser anti-satellite systems has advanced significantly, but never reached levels where an effective weapon could be fielded, particularly if efforts to harden against laser energy are taken into account. The combination of brightness and atmospheric correction needed have been too much to overcome, but given the advances to date I believe this capability could be fielded in the timeframe of interest. A laser ASAT will likely operate from a fixed location and represents a high value target to an adversary. Mobile systems are possible; that feature would dramatically increase survivability. An advantage of a laser ASAT is that it can conduct many engagements over time, particularly against LEO targets. This feature makes such a weapon potentially very cost effective.

Military Support Systems: We have systems in space to support other domains. These are all enduring needs.

ELINT and SIGINT Collection, Analysis, and Dissemination: In addition to peacetime intelligence collection, ELINT and SIGINT systems can provide tactical targeting support to ongoing operations and information critical to EW systems. A future space domain warfighting construct would include survivable versions of these systems and equally important, the ability to process the information they collect into operationally relevant data and information at operationally valuable speeds. Some collection will also be done with terrestrially-based and airborne systems. All of these systems should have the capacity to promptly go from raw intelligence to battlefield situational awareness as to geolocation and identity. They should also support prompt counter-measure development with a high degree of automation. Data analytics and machine learning are important components of these future capabilities. Perfection isn't achievable, so sensors and processing should be designed for the highest payoff practically achievable operational benefit, with increasing performance over time. Current capabilities are far from the achievable goal.

Missile Warning and Tracking: Operationally useful missile warning must be survivable and made available in near real time for warning, for defense systems, and for counterstrike decisions. Threat systems of interest include long, intermediate, and short-range cruise and ballistic missiles including hypersonic missiles. Tracking from origin and during flight will be needed to support defense system engagements on compressed timelines. I'm not convinced the systems currently planned are adequately survivable to support this mission. Similar functionality for longer range air-to-air missiles is highly desirable, if achievable.

Position, Navigation and Timing (PNT): As mentioned elsewhere, this functionality has become ubiquitous and is essential for current systems with a wide range of functionality. The timing service provided by GPS is essential throughout the military services and the current constellation in MEO is more vulnerable to attack than most realize. The latest improvement, GPS III with the M-code waveform, will not be adequate against advanced threats in the future. While providing this service from orbit is by far the most cost-effective approach in peacetime, it creates serious operational risk in wartime. Future space domain concepts should include this service, but acceptable and more survivable alternatives and provisions for graceful degradation if space-based PNT is lost will also be necessary.

Complexities

Fundamental Space Domain Operational Needs

Actionable Timely Attack Warning: The military uses something called indications and warning (I&W) metrics to project the likelihood of an attack and to detect situations in which that likelihood is increasing. For conventional operations, these include logistics movements, exercises that could conceal mobilization or attack preparation, and key leader behaviors. We will need a combination of intelligence indicators, space and ground activity monitors, and artificial intelligence-based data analytics to measure and assess the space operational environment continuously. This is an obvious application of some forms of advanced data analytics and inference machines, but it has to be well supervised by humans and spoofing or deception is a major concern. This type of system can be used to decrease the instability discussed above, but it entails risk. Mutual confidence building measures may be part of this construct, if they can be negotiated and verified.

Command, Control, Communications, and Battle Management (C3BM): During the Obama administration we moved forward with the creation of a joint space operational center, now known as the National Space Defense Center (NSDC). The NSDC is intended to coordinate defense, intelligence, and commercial space activities. The more recently formed Space Development Agency (SDA) is starting to move forward with a "transport layer" constellation to provide communications services to national security space assets. These are steps in the right direction, but my sense is they are small ones compared to the need. There is some danger these initiatives will give us an unwarranted sense of security. In the future, if not now, we will need truly integrated and survivable C3BM for space assets under a single unified wartime commander and we will need communications networks adequate to support both our space-based services needs for data movement and our communications needs for space situation awareness, control of our space assets, and conducting offensive and defensive operations in space. This system should be designed for graceful degradation under attack, very high levels of cybersecurity, and with as much preprocessing of data as practical in orbit to reduce bandwidth requirements. The C3BM system should have highly automated operational analysis tools for assessing situations, evaluating options, and recommending courses of action.

Launch and Ground Control: Our ground control sites are fixed and have significant operational footprints making them subject to adversary targeting. In the future, we will need to acquire launch systems that can be survivability-based, probably through mobility and concealment, and tailored to the classes of payloads (small) and orbits (varied) we intend to utilize for national security missions. We will need an inventory consistent with our expected wartime needs. Ground control systems will need to be similarly robust, redundant, and survivable.

Logistical Support: There are nascent efforts ongoing to provide on-orbit logistical support to satellites. It's an open question, in my view, whether this makes sense for warfighting assets. It may be cost effective to refuel, repair, or augment satellites already on orbit in peacetime. But, if we plan to conceal military assets in space, visibly servicing them is problematic. If we expect our satellites to have short operational lives because of threats, then acquiring the capability to service

them in orbit may not be cost effective. I'm open to the possibilities in this regard, but not certain of how the trade-offs are likely to come out.

Multi-Domain Considerations: Space supports all the other domains and the existence of support from space or the lack of it can be decisive in all other domains. For air, land, and sea surface operations, space systems provide critical situation awareness, warning, and targeting information. Space can also provide secure directional communications needed to support operations in all other domains. Even for undersea systems, connectivity from the sea surface onward will be through space systems. Today, we also have a strong dependency on space for Positioning, Navigation, and Timing for the other domains. While positioning and navigation can often be provided to acceptable levels for many purposes by other means, our dependency on space for high fidelity time references and synchronization is ubiquitous and essential in all domains except subsea, at least for current systems. Space operations are of course dependent on land, sea and airborne C3BM nodes and launch facilities as discussed above. I don't foresee conventional weapon effects being generated from space any time in the foreseeable future (the absentee ratio and launch costs are prohibitive). Currently, the U.S. military services are all wrestling with how to define JADC2 and MDO—today's ubiquitous buzz words. The concepts I have described in earlier sections are very dependent on these space-based functions and associated C3BM.

Space Surveillance and Situational Awareness: As space has become more congested and the mix of debris and small satellites has increased, it has become increasingly difficult to track and monitor all objects in orbit. Throw into this the potential for threat intelligence collection, hard or soft interference by adversaries, and deceptive objects deployed for a variety of reasons. The range of space surveillance needs span continuous launch monitoring, space object tracking, awareness of maneuvering in space, and any proximity operations. Those are peacetime needs. In wartime, add attack detection and characterization and damage assessment. Also, add the requirement for survivability.

Strategic and Tactical Reserves: By strategic reserves I mean those needed for a longer conflict. By tactical reserves, I mean those needed immediately to support the initial stages of a conflict. Reserves can be terrestrial or on orbit, but they must be survivable in either case. This is as much a question of when reserves would be released as it is a distinction about the nature of the payloads and launch vehicles or weapons. Reserve considerations apply to both space defense and offense systems.

Tactical Mission Variations: The future concepts I've described attempt to deal with a scenario in which an all-out surprise attack on our space assets is possible and in which we seek the capacity to launch such an attack on our adversary. One can imagine scenarios in which something less is needed or desired. Three examples come to mind. First are steps to control escalation with actions short of physical destruction such as cyberattack or electronic warfare attack on specific assets. Second is a destructive surgical attack on a specific unacceptable threat capability such as a space-based ASAT directed energy weapon. Third is a defensive operation to defeat a potential set of attackers in the process of moving into position for a future attack. In these and other situations, it would be highly desirable to have a range of options available for national decision makers.

Target Identification/Collateral Damage Avoidance: The biggest operational concern from a cost effectiveness point of view is to use the inevitably limited number of counter-space weapons in the U.S. inventory to attack actual targets as opposed to decoys or non-threatening civil and commercial systems. Given the potential opportunities to conceal or disguise threatening military systems in space and the advantages that might provide, this is a real concern. It drives the need for high fidelity intelligence collection, including on-orbit collection. The collateral damage problem in space is generally not civilian populations,[56] but damage to civil or private space systems and to assets belonging to neutral parties. This can happen through intended but mistaken engagements of targets or through unintended collateral damage from debris or imprecise lethal and non-lethal mechanisms. In a great power conflict that might be viewed as existential; I doubt these concerns would constrain our adversaries, and they might not constrain the U.S. for very long, but they should be taken into account in the design of the future space concept.

Design Requirements and Considerations

Commercial and Third-Party Space Considerations: Many nations and more and more private companies operate space-based systems. There are a host of policy issues associated with the prospect of high intensity military operations in this environment. A future space warfare concept has to take into account the potential for threat systems to hide among commercial or third-party constellations. It must take into account the potential for an adversary to rely on military functionality (intelligence collection, target identification and tracking, communication, PNT) provided by neutral nation states or through globalized corporations. This is as much or more a diplomatic problem or a policy problem as a military design issue, but if the diplomatic and policy problem is not solved, the military problem will be much more challenging.

Confidence in Automated Behaviors: Most behaviors in space are already automated, once a command is given, but that's for local short-term behaviors. The big problem I see here is the lack of time for human involvement in the many operational decisions that would have to be made on highly stressing timelines to fight a determined adversary trying to execute a well-planned coherent attack operation against our assets in space. Selecting a generic option or class of options and enabling automated execution would be all that was possible for humans to achieve, at least without high risk of failure. I am imagining a Pearl Harbor-style attack, combining decisive scale and surprise, because I think that's the best option for an adversary. Why would an adversary do anything else? The only way to gain confidence in the automated operational response we would need is through extensive simulation and war-gaming. Elements of a response, and local behaviors (maneuver or deploying countermeasures for example) could be verified in orbit as well as in hardware and software in-the- loop-simulations, but a large-scale response could only be verified in simulation.

Constellation Management: The task of keeping a large complex constellation of satellites functioning as a unit is non-trivial. The constellations that have been proposed by the Space

[56] Civilians could be implicated in attacks on ground-based space infrastructure. There will be some civilian activity in space itself, but I don't foresee a significant human presence in space in the timeframe of interest here.

Development Agency will need continuous management, as will the proliferated commercial constellations currently being fielded. This function becomes much more challenging when the constellation is under attack and some subset of its assets is destroyed or disabled. This function can be automated—in fact, to a large degree, it must be. The automation for war-fighting situations will need to cope with a wide variety of conditions an enemy may try to impose.[57]

Countermeasures: There are a range of defensive features that should be considered in each space system design. These include maneuver, decoys, self-defense, signature management, and hardening. As satellites increase in mass, the ability to include some countermeasures effectively tends to decrease.

Cyber and EW: These are absolutely an important part of the equation with major design implications for both offensive and defensive space systems. All satellites depend on software and hardware subject to attack at any time in the product life cycle, including in orbit. For any satellite system, there is likely to be a range of potential target portals. Satellites depend on radio frequency or laser communications and a variety of sensors for mission performance and command and control. Ground systems can also be a critical node and a single point of failure in an EW or cyber-attack.[58]

Debris Generation and Avoidance: There is military value in being sure a targeted system is actually destroyed. Kinetic systems with highly visible and conclusive damage mechanisms provide this, but in space, a high-speed collision or explosive weapon is likely to also create persistent and growing debris fields that threaten everything in their orbital paths. Soft-kill can be very cost effective but may leave unanswered questions about the actual status of the target. There is no perfect solution here, but, when possible, debris generation should be avoided—even for hard-kill systems. For some systems, debris sensing and avoidance may be feasible and cost effective, but I have not seen any designs that attempt to achieve this and I'm skeptical it can be accomplished. Sophisticated Space Situational Awareness systems can provide warning for larger items.

Default Behaviors—Loss of Contact/Control: All satellites have provisions for default behaviors in various circumstances. Generally, they are designed to preserve functionality and create opportunities to correct any on-board problems. This is a little more complex for warfighting systems that may be under attack as opposed to experiencing a malfunction, but the design considerations are similar. Depending on the operational profile for the satellite and system and the expected reliable design life, some degree of redundancy and enhanced resilience is likely to be cost effective for warfighting systems.

Energy: I don't see a need for novel energy sources for the space domain, but any technology that matures and has operational, economic, or environmental benefits would be adapted. A number of

[57] An example is an attempt to blow a temporary "hole" in a missile warning constellation so that an attack can proceed without being detected or characterized.

[58] One of my biggest headaches in government was the ground control software program for GPS III, a system called OCX. The driving technical issue causing extensive cost and schedule overruns was cybersecurity.

technologies for propulsion and/or energy generation and storage are in some stage of development. Concepts like on-orbit refueling could also be utilized if proven to be cost effective.

Ground Station Resilience: Ground stations or terminals in general can be an Achilles heel for space systems. Especially for forward located militarily important ground control systems, there should be mobile survivable back-ups in addition to any fixed facilities. Hardening and/or concealment and deception should also be considered.

Escalation Control: While I believe we should take a large-scale attack seriously, one can argue that less decisive attacks in space could be used as part of an escalation control ladder meant to deter the United States. Attacks that do no permanent or visible damage and are reversible are particularly attractive for this purpose. This should be a consideration in our offensive and defensive concepts.

Hardening Options: Physical hardening of space assets against kinetic attack isn't feasible, but some hardening can be designed in for other weapons. Hardening can be achieved against laser attacks up to a certain level through mechanisms like shutter control for optics or reflective non-absorptive materials. Hardening against high power microwave and electro-magnetic pulse (generated by high altitude nuclear detonations) can also be accomplished.

Humans—Locations, Role of, and Support To: I'm not projecting any need for human warfighters on orbit. On the surface or possibly in the air they will be needed for command and control and for key decisions about implementing automated operational courses of action. Because of the operational importance of space, I would expect specialists in space systems and operations to be deployed in the most forward C3BM elements that oversee joint and combined operations as well as at headquarters dedicated to commanding and controlling space operations overall.

Identification Friend or Foe (IFF): Space is big, and movement is constrained by orbital mechanics. Most objects, especially friendly objects, are known to their operators and controlling national organizations—for the U.S., it's the US Space Command. At first blush I'd guess IFF may not be needed or cost effective because of the infrequency of encounters between a friendly and an unknown, but in fact friendly or neutral satellite. IFF systems for aircraft are primarily there to prevent mistaken engagement of friendly or neutral aircraft. Traditionally, they involve active interrogation of a potential threat and require a cooperative response system on any non-hostile interrogated platform. IFF exists for aircraft because airspace can be crowded even in wartime and Air Force pilots don't like the idea of being shot down by an Army air defense system (such as the one I operated in West Germany the '70s). Depending on what mix of military and commercial systems, self-protection measures, and the mix of tactics and threats we expect to field and encounter, it's conceivable the ability to interrogate or self-identify to an approaching object in space would have some value.

Interoperability: The biggest interoperability issue for the U.S. within the space domain is the separation between intelligence and military space assets. More broadly, there are also interoperability needs associated with integration of airborne, terrestrial, and space-based systems as well as with allied systems and commercial systems. The barriers to interoperability are much

more about management, cost, and organizational incentives and culture than technology. The concepts I've laid out are very dependent on the efficiencies associated with space-based targeting and engagement support, assured communication, and PNT support; interoperability for those tasks isn't optional or nice to have—it's essential.

Launch Services: Current launch services are provided by commercial firms and span very small payload capacity to LEO up to very large payload capacity to GEO and beyond. They also provide efficient ways to move multiple smaller payloads into LEO and other orbits. The concept for the space domain requires the additional support of survivable and responsive launch services for payloads for reconstitution of disabled or destroyed orbital support systems. I expect this to mean road mobile and/or aircraft launched systems capable of nominally putting one- or two-ton satellites into LEO. The commercial launch community, currently well populated, can supply some of these needs, but not all. Some wartime capability may have to be provided by military operated systems. Large scale fixed launch locations used for national security launches in CONUS may well be targeted with long-range conventional weapons.

Legal Constraints: The major constraints today are the bans on weapons of mass destruction in space and the possible legal liabilities of creating large debris fields that can damage third party assets. Neither of these is an effective constraint on the concept I've described. There are also legal treaty limits under the Outer Space Treaty of 1967 on militarization of locations like the moon. The practical extent of those limitations is currently being explored in the courts, but they probably don't apply to the concepts described here. There is some international and domestic policy interest in constraining weapons in space and ASAT systems, but I don't see it gaining real traction in the form of international agreements. There is also fairly widespread interest in defining acceptable norms of behavior in space, with or without legally binding agreements. These might include prohibitions on proximity operations and rules about deconfliction and debris creation.

Mission Planning Including Dynamic Replanning: Planning space military operations, largely a mix of satellite attacks and defensive measures, will be a complex endeavor, even before the enemy makes its first move. Once both sides are actively conducting combat operations, it will become even more important to have developed an automated and sophisticated course of action engine that can create and evaluate multiple integrated options in an operationally viable time scale. If we are able to survive an enemy first move in space, U.S. space forces must adapt a dynamic replanning at scale approach as well.[59]

On-Orbit Servicing: This should be considered for inclusion in the concept, but I'm not 100 percent sold on it at this point, at least for military satellites in wartime. On-orbit servicing pays for itself if the extended life and functionality of the satellite is worth the cost of the service. If it makes sense on a cost basis in peacetime, then it should be included for that reason, but servicing during a conflict involves some additional trades that don't obviously support the concept. However, once on-orbit servicing buys its way onto the concept for peacetime, the delta cost for a warfighting capability should be small. Servicing can take a number of forms, but it's often refueling,

[59] An overused and ill-defined phrase in US military circles right now is "the speed of relevance." This is one of many "use cases" where unassisted human decision-making is incapable of acting effectively at that speed.

replacement of a failed module, or movement to a new orbit. I doubt that repair of battle-damaged satellites would be cost-effective.

Operationally Responsive Space: This concept has been around for a long time. It has received support from the Congress to keep it alive over the years, but very little within the Air Force until recently. That is changing now, but we have much further to go down this path. Given the current and projected threats to our space assets and ground-based infrastructure, we are likely going to need operationally responsive space in the forms of responsive launch, war reserve payloads, and payloads that can be activated as soon as they are on orbit. All of this is necessary to support the concept I have described above and to make it operationally resilient.

Operational Planning and Rehearsal: Our capacity for planning and rehearsal in the future will become much more sophisticated and high fidelity. Some forms of Artificial Intelligence will play a major role as we are forced to rely on simulation and autonomy for planning. Rehearsals will be virtual of course, but as we get into actual operations it will be important to learn from real life experience immediately and feed that data into machine learning contexts to improve planning.

Physical Security: A future space warfighting force will need adequate physical security for terrestrial systems. The U.S. will also need physical security for on orbit assets, but it's an open question of how much and in what form. The threat I'm concerned about for our on-orbit systems is peacetime preparation of the battlefield activities by potential adversaries. They will be motivated to conduct proximity operations to gather intelligence, covertly damage our systems, or implant malicious devices (digital or physical) on them for future use. Protecting against these threats should be a design requirement for future systems. Both passive and active security measures should be considered and an enforceable declaratory policy about threat proximity operations should be part of the package of security measures.

Reliability: The cost of US military space systems has been driven by stringent reliability requirements. The cost of the spacecraft themselves, the cost of launch, and the lead times associated with new space systems have all argued for very high reliability in the past. As launch costs have come down and as commercial payloads have proliferated, this equation has changed. Designing for reliability in space is also much better understood now than it once was. The potential for attrition and even high loss rates in wartime is also an argument for reduced reliability requirements. My sense is we will still want high initial reliability, especially for wartime reserves, but less required lifetime in orbit.

Requirements Creep: Conscious attention should be placed on avoiding cost imposing marginal or low return on investment requirements. The natural tendency in all domains, including space, is to add more and more requirements to the design until the concept crashes from its own weight. A lot of the items on this list are good examples of potential requirements creep if not managed carefully. The whole point of all the concepts is improved cost exchange ratios over current systems. In space, we have an environment where the previous assumption of impunity permitted us to ignore cost exchange ratios. That assumption is no longer valid.

Responsive Threats: There will be an action and response paradigm in space as there is in other domains. The U.S. has much more operational support mission capability on orbit today than its potential adversaries but is probably behind in terms of offensive and defensive capabilities relative to space threats. As the U.S. moves to match and exceed what our potential adversaries are doing, it can expect first increasing numbers of offensive systems followed over time by more sophisticated and lower cost per kill ASAT concepts, across the suite of options available. On the defensive side, the U.S. should see efforts to conceal space-based capabilities, use of third-party commercial alternatives globally to support military operations and complicate US planning, and continued use of airborne and terrestrial alternatives to space, including high altitude long endurance UAVs. Both Russia and China are less dependent on space than the US because they expect to conduct operations close to their own boarders. A mutual denial of space-based assets could benefit both relative to the U.S. and might be a more than acceptable result from China or Russia's perspectives.

Secure Communications: This is a necessity for space-based operations and for support to other theaters from space. I expect continuing advances in the relevant technologies, both RF and laser based. Quantum based phenomena are starting to emerge, offering enhanced security from both interception and decoding as well as very high data rates. I'm not convinced at this point the communications architecture currently envisioned will be adequate to deal with responsive threats and provide the reliable communications services future space domain warfighting concepts will need.

Single Points of Failure: For space in particular, our adversaries will actively search for an Achilles heel in the system. Any vulnerability in the C3 system is a potential catastrophic problem. Ground control system nodes are a particular concern. Given the importance of space situational awareness sensors for threat detection and identification, reliance on a vulnerable set of ground and space-based assets for that function could be problematic. The idea of warfighting in space is so new and unique, and its importance is so high, extensive independent red teaming to detect and help eliminate cheap catastrophic attack options is a necessity.

Training, Experimentation, and Testing: A lot of future warfare will be unprecedented and vastly different from our historical experience. This may be most true with regard to conflict in space. The U.S. and its adversaries will all have to rely on the training, experimentation, and testing that can be conducted through simulation anchored in a limited number of experiments. This will put a high premium on accurate modeling and simulation. Equally importantly—perhaps more so—it will place a high premium on the willingness of senior military leaders to accept what the models and simulation are saying about the likely outcomes of future conflicts. My experience has been a general reluctance by senior military leaders to except modeling and simulation results that don't conform to institutional preferences and intuition. This tendency could prove very dangerous, especially when applied to the decisive domain I expect Space to be.

Weather Implications: The main design concern here is the well know problem of space weather, especially the environments associated with high sunspot activity levels. It's a fairly predictable phenomena space system engineers are well familiar with. One would like to avoid a predictable

and potentially exploitable transient vulnerability brought on by space weather. Terrestrial weather is also a factor in requirements for almost everything in the concept I have described. It drives some sensor requirements and affects launch systems and ASAT systems for example.

Other Needed Military Functions

Disaster Relief and Humanitarian Assistance Support: Military space systems can provide a wealth of information in support of disaster relief and humanitarian assistance. There are and will increasingly be a number of civil earth monitoring systems fielded by various states and agencies, so the role of military systems will be to support and augment those in existence for civil purposes. There is a balance to be struck between revealing military space surveillance capabilities and supporting civil functions like disaster relief. This balance should be considered during architecture and constellation design when marginal changes that would be problematic later can be incorporated relatively inexpensively.

Intelligence Support and Support to Intelligence: At this time, I feel there is likely to be a future division of labor between U.S. intelligence and U.S. military space that is going to result in separate systems operated by each to collect similar information for different purposes, on different time scales, and with different degrees of fidelity and resilience. This division is driven by the fact the military needs less precise but more timely and survivable operational support from space while the intelligence community needs exquisite quality products for peacetime national intelligence purposes. While we had impunity to operate in space, intelligence and military needs could be satisfied with the same space systems, at least up to a point. For decades the military has depended on the Intelligence Community to field certain types of space systems, often co-funding systems with mixes of National and Military Intelligence Program (NIP and MIP) dollars budgeted by each community. It was discovered decades ago that very sophisticated national intelligence assets could not connect to and support operational needs in a timely manner, if at all. As a result, there has been some success over the years in ensuring IC systems procured and operated by the National Reconnaissance Office or others could provide operationally useful data to military users in theater. This was acceptable until the advent of robust adversary anti-satellite inventories. The U.S. has the choice to make the IC's space systems survivable enough for wartime use, and to possibly reduce the fidelity of information peacetime users demand, or to create separate peacetime collection and warfighting space ISR systems. At this point, I'm of the opinion separate architectures will be needed, but that decision has not been taken and will be resisted by both sides as long as possible because of the cost and/or potential loss of resources it entails. Whether this occurs or not, there is an enduring need for both communities to support each other, in peacetime and in wartime. That connectivity and cooperation should be designed into any future space architectures.

Missile Warning—Regional: The U.S. has alliances and close relationships with many nation states that are threatened by missile systems operated by hostile neighbors as well as forces deployed forward around the world. These threats are only going to grow in severity in range,

quantity and especially accuracy.[60] Some of the nation states threatening our allies already have nuclear weapons and others may in the future. Our space systems should have the capacity to provide timely direct warning and attack assessment, and possibly engagement support, to global partner countries most concerned about these regional threats and to our regionally deployed forces.

Position, Navigation, and Timing (PNT): I discussed PNT above as a core military capability, but it's much more than just that. It's impossible to overstate how ubiquitous and important PNT services are to both the military and civil communities. GPS and its several global clones are used throughout the world and in myriad applications, many of which are not generally recognized. The U.S. military will undoubtedly continue to provide this global service in peacetime indefinitely and it will continue to modernize PNT services including adopting more security against threats like jamming and cyber-attack. PNT will also continue to be a lucrative target for our adversaries and potentially an adversary vulnerability the U.S. can exploit for its own purposes. I don't disagree with the need to take steps to protect GPS, but I believe the U.S. should aggressively pursue alternatives and back up capabilities to GPS for military systems in general and possibly for civilian use. We can't afford to be completely dependent on one system for such crucial services.

Special Operations Support: Military space systems should be integrated with other stand- off systems that support special operations such as counterterrorism and counter-proliferation. The last two decades of emphasis on counter-terror have led to tight integration of relevant national capabilities and this should continue for the full range of future special operations applications as new systems focused on great power competition are fielded.

Weather Sensing and Forecasting: Commercial and civil space-based weather monitoring and predicting systems have become more and more sophisticated and detailed. As this has happened, the demand for military specific space-based weather systems has diminished to almost zero.[61] The trend to ever more precise civil weather forecasting and monitoring is certainly going to continue, especially as more severe weather events occur. The problem for the military will be the availability of this information during great power competition. Future architectures designs should take into account the potential that at least some of the national and internationally sourced weather information may not be available during a conflict.

[60] Israel is a good example. I've been in Tel Aviv for rocket attacks and once spent time in a hard room with the Israeli Minister of Defense during an alert. Israel's defense systems like Iron Dome have coped adequately with current threats because the attacking rockets are unguided and only a small percentage have to be intercepted to protect populated areas. Once Israel's enemies acquire precision missiles the equation will change completely.

[61] There are some unique military needs such as more precise sea surface winds, better cloud cover predication, and data related to local off-road ground mobility. In tight defense budgets there hasn't been much willingness to pay for systems to obtain this information, however.

Warfare Domains – Cyberspace

Introduction

I decided to categorize cyberspace as a separate domain because I believe we need to think about cyberspace as an analogue to the other domains of warfare, all of which are geospatially distinct and each of which has its own environmental characteristics which are determinative of how conflicts occur in those domains. All of the domains I'm describing are related to one another and interdependent. Warfare doesn't respect human definitions of boundaries—it's a very pragmatic endeavor. Like EW, cyber operations will take place in all the geospatial domains. That aspect of cyber, like EW itself (which I am not treating as a separate domain), must be dealt with in the context of conflict in the geospatial operational domains.[62] The operational cyber threat dictates cybersecurity be a high priority in every domain and throughout the whole spectrum of operations and support functions. It also provides some potential opportunity for decisive defeat of an adversary through military operational cyberattacks. It is a given to me that future military systems across the board must be designed to be cyber secure and resilient to cyberattack. The U.S. also has to do its best to prepare and field cyber offensive weapons targeted at adversary military systems and functions. I'll discuss this use of cyber briefly, but it's not the reason there is a separate cyber domain section of this paper.

Here, I want to distinguish strategic coercive cyber warfare from cyber operations conducted in support of conventional military operations and to focus on this distinct class of cyber conflict. One can think of strategic cyberwarfare as more than just a domain; it's a whole new way of using a certain type of force to coerce an adversary into desired behaviors, or to even force capitulation. The best analogy may be to the way strategic air campaigns were thought of by some theorists in the 1920s and 1930s as decisive means, on their own, to compel an adversary's behavior. The idea then was wars could be won by strategic air campaigns alone, using conventional bombing to effectively bludgeon a nation into capitulation by destroying the infrastructure of the country and the ability of its economy to support conventional warfighting and society.[63] Conflict of this type in the strategic cyber domain can be either independent of or combined with conflict in more traditional domains. I have a hard time conceiving of a conventional conflict between major powers in which strategic cyber warfare is not part of the equation—by both sides. Before I jump into that concept, let me start with a few words about cyber in support of future (or even current) conventional military operations.

Like EW, military (or if you prefer, tactical) cyber operations will be ubiquitous and cut across all traditional military domains. I've covered that aspect of cyber as a "complexity" in the other

[62] There is an argument that the struggle for control of the Electromagnetic Spectrum should be treated as a domain. I didn't take that approach because I don't see this struggle as separate from warfare in the domains I have discussed. For cyber, I'm focused on cyber in this section as a place of conflict independent of the other domains I address.

[63] Although it has been disputed, one could characterize the NATO air campaign against Yugoslavia as a successful example of a bombing campaign alone forcing a state to capitulate. The degree of dominance NATO had in this campaign was completely overwhelming.

domains. Every weapon system, all C3 systems, and all logistics support systems, as well as the commercial networks and nodes they connect to, will have to be designed for cybersecurity to be effective in wartime in the context of conducting and supporting conventional military operations. Legacy systems which have been in the inventory for decades in some cases, are often the most vulnerable to cyber defeat. Military cyberspace offensive systems will be developed and employed as part of the spectrum of military capabilities any advanced nation state fields. Conventional military cyber has some characteristics that are important to recognize and understand, and to distinguish them from what I'm calling the strategic cyber domain.

To be effective, conventional military cyber should be used in close conjunction with conventional military operations. Some degree of destructiveness can be achieved with cyberattacks alone, such as taking control of and de-orbiting an adversary's satellites, or in taking over a UAV's flight controls and causing it to crash, or even in redirecting a weapon to attack its own forces. However, most conventional cyber military operations, like EW, will be used to degrade an enemy's weapon systems or C3 systems in order to enable a more successful conventional attack. Cyber vulnerabilities are fragile; they can generally be readily corrected once they are known, and a successful attack creates only a transient advantage. In general, attacking cyber military vulnerabilities buys the attacker some time. Coordination with kinetic operations must be timed to exploit that transient advantage. Cyber vulnerabilities can be exploited through a synchronized conventional kinetic attack of some kind. That attack must be conducted while the cyber attack's effects have not been corrected.

Cyber advantages are also unreliable. An adversary may identify and correct an existing cyber-vulnerability at any time, the attacker's access may be cut off, or deception may be used to create the false belief a vulnerability exists where one does not. Tactical cyber advantages are opportunistic. They depend on the enemy having an exploitable weakness in one or more of his systems. The attacker must find and exploit those weaknesses where they happen to exist. The attacker may also not be able to determine with confidence the success or failure of a cyber-attack, creating uncertainty and risk. All that said, cyber can certainly be decisive in support of conventional military operations but relying upon it to be decisive or to create an enduring advantage is a high-risk approach. In the conventional military domains, cyber will be an adjunct and complement to more conventional destructive military force.

The strategic cyber domain is concerned with using cyber-attack, independently of other forms of warfare, as a coercive mechanism in its own right. This idea isn't entirely new. During the interwar years of the 1920s and 1930s there was a vigorous debate about strategic bombing campaigns, their potential to break the will of an adversary or their ability to efficiently destroy an economy's capacity to support both a population and a military enterprise. If successful, proponents asserted, strategic bombing could eliminate the need for traditional ground campaigns and even dramatically reduce the destructiveness and cost of war itself.[64] That debate is still active in some circles. The

[64] Malcolm Gladwell's recent book "*The Bomber Mafia*" captures this debate and how it resulted in the strategic precision bombing campaigns against Germany and Japan in WW II. Notably both campaigns ended in massive casualty producing attacks on population centers, as opposed to the limited precise and high leverage strategic targets theorists had envisioned as decisive.

strategic bombing air-warfare theory was tested in the WW II air campaign in Europe in particular, with mixed results at best. The conventional strategic bombing campaign against Japan would not have obviated the need for an invasion and was decisive only with the introduction of nuclear weapons. The strategic air campaign idea was that a nation could be coerced by the physical destruction of economic networks and transportation networks interior to the state, forcing capitulation or overthrow of the sitting government. The same target sets and more are susceptible to a strategic cyberattack.

A lot of what I've written in this paper addresses the potential to remove human beings from direct combat through lethal autonomous systems. Strategic cyber-offensive operations finesse even that development, and possibly even the need for offensive conventional warfare itself, by putting populations and their governments directly at risk of catastrophic collapse through disruption or manipulation of their digital systems. I can't predict if strategic use of cyber would be successful in the future, but I can predict that it will be attempted; it's already being used by our adversaries. Like military or tactical cyber, it will also be used in conjunction with conventional military operations as well as independently.

Modern societies and modern governments are almost completely dependent on the flow of information through digital networks and on the processing and storage nodes they connect. Most wealth today exists only in digital form. Technology, innovation in business concepts, and economic imperatives are going to continue the movement toward an ever more digitally integrated and interconnected world. For the foreseeable future, there will be a profit driven bias toward improved services, products, and efficiency over security. Security in the form of resilience has certainly improved, but absent some compelling event, cyber-security will always be playing "catch-up."[65] For a nation prepared to make the investment in offensive strategic cyber, this presents an opportunity to create a very powerful, and unprecedented, coercive capability. We are already seeing cyber disinformation campaigns designed to influence the United States, to weaken the government's legitimacy, and to amplify and distort internal divisions. We are also seeing extensive theft of data, especially intellectual property and personal information (financial and otherwise). There have been reports of malware found in critical infrastructure, such as power grid control systems and ransomware has been used to temporarily shut infrastructure systems down. The capability I'm describing here goes beyond, but not far beyond, what we have seen or experienced so far; it provides the capacity to overtly compel a foreign state to affect a desired behavior through either cyber-attacks or cyber-blackmail, independent of other means of coercion.

How would one use this capability in practice? I doubt it could be used to force a nation to capitulate completely, allowing occupation and regime change for example. Nations will endure a great deal before reaching those points. The threat of nuclear retaliation, for a nuclear power at least, would also conceivably limit the attacker's objectives to ones the threatened state could accept. For example, strategic cyber could be used to prevent a response to an act of aggression

[65] Richard Clarke, who years ago sounded the alarm about cybersecurity vulnerabilities has become more optimistic in recent years as cybersecurity as a discipline and cybersecurity products have improved. See *Cyber War*, 2011 and *The Fifth Domain*, 2020. My own conversations with cybersecurity experts suggest that Clarke is too optimistic.

against something that was not seen as a vital interest. It could also be used to force a nation state to change its international behaviors, reduce its forward deployments, or adjust its international policies. Any use or credible threat of use of strategic cyber would likely trigger a response that would reduce vulnerability and increase counterattack capability. This provides some, but only limited deterrence to use. The most attractive opportunities for cyber-coercion will be situations in which the aggressor places a much higher value on its objective than the threatened state does. There are plenty of examples, but the reunification of Taiwan with China would be on that list.

One other important potential use of strategic cyber is by a less capable adversary seeking to deter a great power like the United States from an expected adverse action. This may be the most likely use of strategic cyber; there would be a strong upside and very little downside consequence, even if the attack failed. Strategic cyber in this context would be seen as an "off-set strategy" against a state, like the United States, that has dominant conventional and nuclear capability. For states like Iran and North Korea, strategic cyber could be a powerful, and very cost-effective, deterrent to intervention by the U.S.

The advent of strategic cyber, just as a possibility, opens up a theoretical can of worms, or if you will, a Pandora's Box, that has to my knowledge not been explored adequately. There may be a body of academic work in this area, but there is no general public or political understanding of the implications of strategic cyber. I won't try to fill that gap here, other than to point out this needs to be done. A great deal of intellectual firepower was expended in the 1950s on the task of understanding what nuclear weapons meant for international relations, future conflict, and the threat these weapons posed to humanity and how to avoid a catastrophic nuclear exchange or event. That effort isn't complete, as a recent work by my friend Bill Perry makes clear, but our understanding has moved forward dramatically since the 1950s.[66] I don't think we have made even a good start at understanding the implications of conflict in strategic cyberspace yet.

Unlike nuclear weapons, which have a clear "used" and "not used" defining boundary, strategic cyber conflict has a continuum of levels and no clear boundaries and no internationally agreed norms of behavior. Questions that should be addressed include: when is a cyberattack an act of war; how would conflict in the cyber domain couple to or trigger both conventional and nuclear conflict; is there a Mutually Assured Destruction (MAD) equivalent for strategic cyber; should there be; is strategic cyber inherently unstable—favoring a first user substantially, if so what could be done about this; how might the laws of armed conflict apply, are there practical forms of legal constraint on behaviors, if so could they be implemented and enforced through international law; is there a meaningful distinction between espionage and attack preparation, or even attack itself; is there a distinction between physical destruction and digital destruction that has any utility in reducing risks of conflict, what would the characteristics of escalation be and could they be controlled. These topics and many others should be deeply explored and publicly debated and there should be some international consensus on them, but for now I'll confine myself to describing future strategic cyber weapons and how they could be used operationally. These could be weapons of the future, or they could already exist.

[66] See "*The Button*" by William Perry and Tom Collina.

Operational Concept

A strategic cyber operation would attack a set of targets, networks, and nodes on networks of high value to the state attacked. They should be systems essential to the functioning of the attacked country and the loss of which would be unacceptable to the threatened government and or population. There are no shortage of potential target sets for a strategic cyber-attack. Integrated digitally connected systems of air, sea, and land transportation, commercial power generation, financial transactions, wealth storage, consolidated data storage generally, and communications systems including public commercial media essential to societal control are all potentially vulnerable. The objective is coercion without provoking a response that is counter-productive—a nuclear counterstrike for example or invasion of one's country. For that reason, scalable effects are useful, even essential. The ability to crank up the gains or to back away by reversing the effects of an attack and on both the degree and permanence of the damage are all of operational value. A combination of serious "signaling" destruction levels with the threat to escalate substantially would be operationally valuable. Unlike everything else I've discussed so far for other domains, where autonomy removes emotion from the equation, this form of future warfare is all about psychological impact on the enemy's population and leadership. The strategic cyber domain isn't just about cost-effective exchange ratios and winning on a conventional battlefield. The goal of the strategic cyber campaign is to force a desired behavior without triggering an extreme reaction – such as a nuclear strike, or an extended conventional conflict. However, if a general or regional war is underway, strategic cyber can complement conventional military actions to help dictate the outcome of that conflict.[67]

It's worth highlighting that because strategic cyber is all about influencing humans, some forms of artificial intelligence play an important role in strategic cyber. An enormous amount of research on AI is about defining how to influence human beings, mostly to buy things, but also to persuade people to accept and internalize political messages. A strategic cyber campaign is as much an information operation as it is a technical attack on digital systems.

A coercive strategic cyber-attack as I would imagine it, starts with the communication of three critical messages: (1) this is what we want, (2) this is what we can and will do to you if we don't get it, (3) resistance is counterproductive and futile. It's simple and straightforward to communicate the first message. If an adversary is applying strategic cyber against the United States, it could be reunification of Taiwan with mainland China, withdrawal of air and naval forces from China's sphere of influence in the Western Pacific, the reabsorption of the Baltic States and Ukraine into Russia, or the withdrawal of US military presence from Europe. The second and third messages are communicated by words and actions. The scale and visible impact of these actions

[67] The will of a population to endure attacks has often been underestimated. In many cases even protracted bombing has only stiffened the resolve of the target population. That can certainly happen with strategic cyber as well.

and communications are critical to success.[68] They must convincingly demonstrate both capabilities and intent.

A strategic cyber-attack must therefore be tailored to the vulnerabilities and culture of the target. For a coercive strategic cyber-attack to be successful it must be perceived as overwhelming, and it must put at risk things of high, even existential value to the defender. The psychological impact of the attacks on the defending government and population is the key to success and this should be carefully analyzed by an attacker. A given nation's vulnerabilities to cyber-attack are likely to be unique to that nation. Both culture and infrastructure characteristics matter. Totalitarian governments like China are very concerned about their control of the flow of information to their populations. Other nations, like the United States may be more vulnerable to specific material disruptions. Crippling any of the various networks mentioned above would have a devastating impact on the population of the United States. When public will to resist is the target, attacks should have visible and visceral impacts on as large a fraction of the population as possible. The attack must be "real" and penetrate the consciousness of the general public at scale. In the U.S., public reactions would be swift for an attack on any of the critical infrastructure networks. One national system that affects virtually every American continuously is the commercial power grid. Taking control of that grid and demonstrating the power to shut it down, including some physical destruction, would have a strong impact that could touch every American. Strategic cyber campaign planners don't have to guess about what would be effective. It's even possible to conduct covert experiments on a target population to acquire data to help AI analytics model the target state's responses.[69] If that's considered too risky, then data on a given society or culture can still be collected by observing the impact of random criminal and nuisance attacks.

In structuring a strategic cyber campaign, it would be most effective to attack several critical infrastructure networks and systems simultaneously. This would mitigate the risk of a failure in one or more targeted networks and have the highest motivational impact. It would substantially impact the attacked nation's ability to respond, and it would sow confusion. If possible, the attacks should be reversible and scalable so relief from the damage can be offered as an inducement, and gradations in severity can be managed to manipulate the targeted society. The more power and control the attacker demonstrates, and the more clearly it communicates there is no easy remedy or "fix," the more likely the defender will accept that resistance and escalation are in its interest. A coercive attack would also be more effective if the potential for extreme damage, not yet inflicted but clearly available, was apparent and credible.

Simultaneous with launching attacks on an opponent's infrastructure, the attacker would need to take steps to harden its own critical networks and functions against a response in kind. Instituting

[68] The recent COVID experience in the U.S. demonstrates the importance of communication to human behavior. Something as straight forward as wearing masks or getting a shot could not be communicated effectively to the American people as a whole. The fact that many people did not personally directly experience the impact of COVID and rejected information sources they didn't trust has powerful implications for how to structure a successful strategic cyber campaign.

[69] Which makes one wonder if the recent ransomware attacks on oil distribution and meat packing in the US had an even more insidious purpose.

a strong national cyber-security program in advance and having the ability to sever, at least temporarily, all connections with extra-national networks would be part of this concept.

Effective intelligence and counterintelligence are essential to preparation for and defense against a strategic cyber-attack. Intelligence depends on network or system access and so does the ability to design and execute an attack. The concealment of the offensive elements of the concept and all the actions to prepare for execution is essential. Given knowledge and time, any prospective attack can be defeated if it is discovered before it is executed. Deniability if attack preparation is discovered is also an attractive design feature. Most defensive measures for counterintelligence could be carried out as acknowledged cyber-defense best practices, but some measures would also need to be concealed.

Offensive capabilities are only half of this operational concept. It may be even more important, especially for the United States, to define the defensive operational approach. How should a nation like the United States protect its critical information infrastructure in the future? This can't be left to the marketplace. The marketplace is too fragmented, and the economic incentives do not motivate businesses and local or even federal governments to invest heavily in cybersecurity. I don't see any alternative to mandating through regulation that all critical infrastructure maintains high standards of cybersecurity. The government should also invest in and define the tools and network architectures, applications, and devices that should be used to provide security and keep pace with the threats. The conventional wisdom is the sophisticated threats will always be a step ahead. That may be true, but I don't accept it as a given. I'm certain the threat will always be well ahead if we don't invest adequately in the various aspects of cybersecurity and require their implementation. In the world of defense against nuclear weapons, with which I have a lot of experience, there is no such thing as a perfect defense. Even so, every nuclear weapon that is successfully defeated matters and the fact of a defense acts as a deterrent. So it is with strategic cyberattacks. Imperfection is not a justification for inaction.

Building Blocks

To acquire an offensive strategic cyber capability, one would first have to build a dedicated cyber-force or cyber-command with this specific mission. Conventional echeloned military organizational models can be applied to the other domains I have described, but with unlimited flexibility as to relationships and unit sizes. Something entirely new is needed here. The mission of this new organization is to create and field a capability to put other nation states critical civil infrastructure at risk in a way that will compel desired behaviors. It should probably have a matrix organization, with one axis being the targeted states and the other axis being technology and target set type expertise. This new military capability is independent of conventional military operations or nuclear operations, so this organization should be independent of the organizations with those missions. This organization, and its mission, should probably be concealed as much as possible, probably with a deceptive cover story. I say probably, because there is some value in having one's adversaries concerned about one's capabilities in this area. The new strategic cyber organization would be responsible for acquiring and operating the following:

Access systems that would provide long term access to foreign networks and nodes would have to be acquired and sustained. It would be expected that over time, some access points would be discovered and closed or diverted into deceptive dead ends. Some would simply age out as technology evolves. Redundant access systems would be highly desirable. As new adversary systems are acquired, new access systems will be needed.

Intelligence and battlefield preparation or shaping tools that penetrate and collect information about foreign networks and systems and that create the opportunities to embed weapons.

Operational weapons that could be used to shut down, slow down, or erase enemy systems would have to be developed on a case-by-case basis tailored to the target set. Weapons with wide capability through broadly used commercial targets, at any point in a commercial stack, are desirable. To the extent possible, reversible and scalable effects would be desired. Some tools could cause irreversible or permanent physical damage (a la Stuxnet). There should be a large and comprehensive inventory of tools with continuously evolving capability against emerging or new technology as it is fielded.

Planning tools including tools to analyze the psychological and emotional impact on societies and leadership would be necessary for "campaign" planning.

Testing infrastructure that would include interaction with humans and human behavior modeling as well as technical testing.

The defensive side of the strategic cyber domain has its own building blocks also. Many of them are mirror images or counterpart of the types of systems and tools needed for offensive strategic cyber. There needs to be layers to any strategic cyber defense systems. The last layers in this chain are the defenses under the control of the organizations operating on the internet, government or commercial. If we are going to have effective defenses, we also need to ensure the networks themselves have layers of effective defense and the ability to detect and respond to attacks. This can be accomplished through regulation of the industries involved or through greater direct government involvement. The Department of Homeland Security is an obvious focus for either approach, but I would guess the bias for the foreseeable future will be for very limited government involvement in commercial networks. Events may change that bias. Whether we like it or not, for the foreseeable future there is going to be an arm race in this area between attackers and defenders. For the U.S., I don't think we can rely completely on the marketplace to generate the defensive tools, architectures, applications, and devices needed, but we can supplement, complement, and motivate that marketplace to be more effective. Government regulation is a building block for defensive cyber capability, but investment is also required. A strong dedicated organization, separate from but coordinating with the offensive organization is needed. In the U.S., the current organizational structure dedicated to this mission is a start, but it is probably inadequate and needs to be reconsidered in light of the need for a stronger government role and more sustained investment. Internationally, nations who wish to lower the risk of this type of threat must work together to develop more effective defensive techniques and tools as well as countermeasures that

can be widely used. The recent Solarium Commission addressed many of these concerns and is a good starting point for outlining a more effective defensive cybersecurity posture for the future.

Complexities

Fundamental Operational Needs

Command, Control, Communications, and Battle Management (C3BM): By its nature, strategic cyber operates on largely commercial networks and dedicated networks that interface with the commercial internet-connected world. C3BM for protection efforts for commercial networks including network infrastructure, data, and functional resilience will be largely a commercial firm responsibility, although hopefully within standards established by the government. Events may force a stronger role for the government in this function, although not necessarily for the Department of Defense. If so, that role will have to be integrated in a C3BM structure that incorporates intelligence, defense, and homeland security, just for starters. Presumably this will continue. The counterattack mission necessitates a strong operational C3BM link between commercial network providers and military responders. By its nature, and due to the importance of time in defense and response, much of this interface functionality must be automated, but there must also be strong human control of responses to ensure those actions are justified and appropriate. In normal peacetime use this function is episodic. There is a background of ongoing malicious activity punctuated by intermittent significant incidents. If a threat mounted the type of coordinated, comprehensive, and decisively coercive type of cyberattack described above, it would require a much greater capacity and scale for assessing and managing a response than the U.S. has, to my knowledge, acquired. The type of C3BM capability needed to support a large-scale counterattack or a large scale offensive strategic cyber operation such as I've described could be acquired today with appropriate investments, if the decision were made to do so.

Logistical Support: To acquire and maintain the type of strategic cyber force I've described would require a continuous pipeline of new attack techniques, means of access, and monitoring methods as well as up to date attack planning and management tools. The world of cybersecurity and cyber-related technology is incredibly dynamic. Any vulnerability will be fixed quickly as soon as it is detected or exposed. Without a robust supply pipeline of new techniques, an existing inventory of attack options will decay over time.

Multi-Domain Considerations: Strategic cyber operations will often be employed in conjunction with conventional military operations. There are good examples of how Russia in particular has linked cyber operations against commercial networks to military and gray zone actions. These include operations against Estonia, Georgia, and Ukraine. A combination of disinformation, denial of service, and disruption have been used in support of military or quasi-military action on the ground in each of these cases. If strategic cyber is used in direct coordination with larger scale military operations, it can provide a very cost-effective alternative to kinetic attack for disabling transportation and logistics nodes for example. Most militaries, including the U.S., are highly dependent on supporting commercial networks for acquisition of supplies, transportation, and personnel management. In most scenarios, the U.S. has to flow people and material overseas on

short timelines and then sustain those forces. All the networks and software systems for managing these functions are potentially lucrative and cost-effective targets. Looking at it from the opposite perspective, the same may be true of our adversaries. There is no need to wait for future technologies to address these risks and opportunities.

Resilient Basing and Operations: Strategic cyber operations headquarters and facilities are basically office buildings and cloud computing environment installations for data storage and processing. In a future conflict they would be high priority targets for any conceivable type of attack. The best means of providing resiliency is probably deception—making them look like all the other similar facilities. A problem with this approach is the potential for a peer adversary to track the people who worked in the facilities and to observe patterns of behavior, including cyber behaviors. A combination of deception and redundancy could be most effective as well as reasonable levels of physical and cybersecurity. In any event, resiliency, for both installations and their functions should be an important design consideration.

Tactical Mission Variations (offensive and defensive cyber operations, surgical strike, raids, interdiction, misdirection, hostage taking/ransomware, and escalation control): There isn't much limit to the types of options a strategic cyber suite of capabilities could provide to national leadership. All the types of attacks the commercial world and governments have already experienced are on the list, and several more. Again, this isn't a technology dependent future; it exists now. The questions about what capabilities to acquire are more about policy and priorities than they are about technology. A caveat is these options can't be instantly available; there has to be an often long and uncertain effort to acquire access, sustain it, and build tools or weapons to exploit any discovered vulnerabilities.

Target Identification, Access, and Exploitation of Vulnerabilities: Before one can develop or launch a cyberattack on a target, it is necessary to find that target and obtain digital access to it. Once inside a target network, it can take significant effort to find and exploit vulnerabilities. This can take years, and access is a very perishable asset once it's obtained. Sophisticated opponents will also take steps to deceive attackers into thinking they have access to a target when they have been lured into a "honey pot" virtual deception. A problem with preparing cyberattacks against a target is the more activity within the target's systems, the more likely discovery will be. There is a very strong tension between intelligence collection needs and cyberattack preparation that may include implanting weapons in an adversary's system where they could be discovered. This work is necessary, however, to the preparation of strategic cyberattack options.

Design Requirements and Considerations

Attribution: A major power trying to coerce a desired behavior through cyberattack or the threat of cyberattack wouldn't normally be concerned with attribution. It would be a virtue. This isn't true for many other cyber operations, however—on either side. Attacks or intelligence collection can originate from anywhere with an internet connection and be routed through a large number of intermediate global locations prior to arriving at the target system. The origins of an attack can be contrived to create false attribution—for any number of purposes. Attribution is a serious problem

for defenders who would like to preempt an attack or mount a counterattack and/or exact other consequences against an attacker.

Anti-Tamper: A cyber attacker generally relies upon concealment prior to an attack and once an attack is executed, the weapon used is assumed to be compromised. This isn't necessarily true, and one can imagine cyber weapons whose functionality includes self-deletion, or some other technique, to prevent an adversary from reverse engineering the weapon in question.

Collateral Damage Avoidance: There are multiple examples of cyber weapons that have ended up harming the wrong target or simply gotten out of control and wreaked havoc once released into the massively connected cyber universe of the internet. STUXNET is one example. In a large scale strategic cyberattack it also isn't hard to imagine significant unintended consequences including loss of life and property. There is even the threat a cyber-weapon will be "captured" and used on the originating nation. None of this precludes the development or use of these weapons, but it implies care has to be taken to understand and limit their effects.

Confidence in Automated Behaviors: Strategic cyber operations, once initiated, will be highly automated by their nature. There must be reasonably high confidence in the net effects of the attack. If threats are used to motivate the opponent, then the attacks must be convincingly consistent with that intent. Full scale testing isn't always possible, but software in the loop laboratory testing is essential, and some limited field testing is highly desirable. Scaling may be straightforward or uncertain and risky based on the targeted system and attack type. Simulations can be used to evaluate scaling performance. Whatever the collection of verification means, the confidence level in a strategic cyber campaign's automated behaviors should be at least as high as that associated with a conventional military campaign.

Countermeasures: Both on the offensive and the defensive side, there are and will be continuing efforts to develop countermeasures and to anticipate and overcome them. Some of these will be as simple as disconnecting from the internet completely and others will involve very complex defensive measures designed to isolate threats, limit damage, and speed recovery.

Deception: Strategic cyber has its roots in the world of espionage and counterespionage, where deception is the norm and can take many shapes. For the U.S. at least, the military community tends to deemphasize deceptive measures; it's part of the doctrine, but not a prominent feature of operations, nor an area receiving significant resources. The intelligence community, in contrast, lives on deception and we should expect it to be a prominent part of designing and operating strategic or tactical cyber systems, for all purposes.

Default Behaviors—Loss of Contact/Control by Echelon: Generally, cyber weapons deployed "behind enemy lines" so to speak are likely to be cut off from our control early in a conflict. A range of default behaviors are possible, as long as the autonomous agent we have deployed still has some degree of control over itself and its environment. Designs should include appropriate provisions for loss of supervision or communication, just as with any autonomous platform.

Escalation Control: Strategic cyber provides some interesting potential for escalation control, or at least the attempt at escalation control. It is certainly possible to construct an escalating and

deescalating series of steps an attacker can use to try to influence the decision making of an opponent. This consideration applies to both sides of the equation. For the offense it's a matter of trying to construct rungs on the ladder of severity and psychological impact that have some degree of predictability. As discussed earlier, AI can be important here, but actual behaviors under stress can be difficult to predict, particularly with strong cultural differences. The range of options potentially available to an attacker is almost unlimited, at least in theory. Couple this with a range of other non-cyber steps and it creates an even richer playing field. A lot can be done to try to control escalation without crossing the line of employing violence against human targets. Examples in the case of China attacking the U.S. include graduated cyber-based disruption of both military and civilian activities (including steps like taking physical control of military or civilian satellites through cyber penetration), plus jamming or even DEW attacks on key satellites. For the U.S. there are potential cyberattacks on the Chinese economy, on military support systems, and on the control the CCP leadership exercises over public access to information. From the defender's perspective, there are a range of actions that could be used to negate or minimize the impact of all of these possible steps and to show one's own resolve. None of these tools will be available in a crisis unless they are prepared ahead of time and included in the strategic cyber arsenal and cyber C3BM system for possible implementation.

Humans—Location, Role of, and Support To: For strategic cyber defense, I would envision an extension of what we have today, which relies upon humans as commercial network administrators and corporate Chief Information Security Officers and Cybersecurity Officers (CISOs and CSOs) and their associated staffs of IT specialists.[70] Law enforcement and intelligence organizations play a significant role today and the federal government has some limited capability through DHS. DOD's role, through Cyber Command, is largely limited to some technical security assistance and counterstrikes against attackers, all of which involve human expertise and informed decision making. Automation will play a major role, but it must be managed effectively by humans. For an effective defense against a well-planned and executed cyberattack, much more will be needed in terms of integrated headquarters and human decision-making capacity on policy, regulation, and preparation. I believe the U.S. has an organizational and a human capital need for more effective defenses, as well as better technical tools, that isn't being met today. The lack of this capability leaves the U.S. with some unattractive kinetic options for deterring and responding to a large scale cyberattack as our default posture. For strategic cyber offense, I would envision integrated multidisciplinary human campaign planning teams for each potential target, with associated sets of AI-based analysis tools to evaluate vulnerabilities of potential targets and assess the impacts of various courses of actions. Given what we have already seen, it seems safe to assume our potential adversaries have already implemented something like this.

Interoperability: At this point, my take is any attempt to build an offensive strategic cyber capability would be U.S. only, at least initially. My view is the risks of compromise currently outweigh the value of interoperability. There may be specific threats and specific cyber weapons where we want to move cooperatively and in some interoperable way with one or more

[70] These are relatively new C-suite positions, and an indication of how serious cybersecurity has become to commercial firms.

international partners, but that should be the exception rather than the norm. Defensive cyber is just the opposite. The US and its close partners should be working together closely on measures to defeat and mitigate the threats to our infrastructure and critical national assets. We should be sharing information about threats and protective measures and working on common security standards. There may be times when these two regimes are in tension, but those issues should be worked out on a case-by-case basis.

Legal Constraints: This is a complicated area where a range of governing laws spanning privacy, search and seizure, criminal, international, and law of war all have potential implications for military operations. In many cases, the implications of existing law in the cyber domain are not well developed and certainly not uniformly applied. To some degree, cyberspace is largely the "Wild West." There is a huge problem today in the inability to enforce existing laws with regard to topics like intellectual property, privacy, data theft and even espionage. The ambiguity about the threshold for a cyberattack to be considered an act of war is rightly or wrongly considered a virtue by many; a clear line would effectively provide a license for activities below that line and would put states in uncomfortable box for actions above it. I expect the U.S. will (and should) make a strong effort to comply with legal constraints on cyber activities. I don't expect this of our potential adversaries. As we plan strategic cyber operations, we will need to take into account any widespread suffering imposed on civilian populations which may be precluded by the laws of war. Absent any international consensus or agreement, we will have to decide for our own planning purposes what level of cyber operation constitutes an act of war, with its concomitant legal constraints.

Operational Planning, Rehearsal, and Dynamic Replanning: Any strategic cyber campaign should be carefully planned, tested in simulation as realistically as possible, and include features that permit rapid response to foreseeable target changes or broader reactions. A secure development and testing environment, with as much realism and the ability to scale or emulate scale will be essential. Digital twins have become a popular concept recently—for strategic cyber weapons a digital twin is needed for testing and performance verification and concurrent development during an operation. In some cases, limited rehearsals or carefully conducted tests may even occur on adversary networks.

Perishability: Cyber weapons are very perishable. As soon as their existence is discovered (or even if it is not), the weakness that led to their creation can be eliminated—almost always through software and/or procedural changes that can be developed and scaled quickly. Even before a weapon is discovered, the vulnerability it depends upon may be eliminated due to routine security updates, other unrelated changes, or obsolescence of the system hosting the vulnerability. As a result, cyber weapons must be continuously evaluated for their effectiveness and newer weapons constantly pursued.

Physical Security: The physical isolation and security of all future strategic cyber related activities is a given. As mentioned elsewhere, strategic cyber-related personnel and facilities will be a high value target for threat espionage, sabotage, and attack efforts of all types.

Psychological Warfare: Strategic cyber is a form of psychological or information warfare in that it is designed to influence human behavior without widespread violence or direct coercion. The design of a specific cyber weapon may be influenced by AI-aided psychological analysis of the targeted society and leadership. The impact of the choices of targets and the choices of effects overall on those targets is highly important. This is the whole basis for a strategic cyber campaign plan. We know some attacks only increase the will to resist. As our ability to understand human behavior improves through AI-based analysis, we should be able to project the impact of a strategic cyberattack much more effectively and precisely.[71] The structure and sequencing of an attack, and the accompanying messaging, as well as the specific content of an attack are all important to success. A campaign can end as soon as the reality of "overwhelming force" and the "futility of resistance" are understood by the targeted society and/or its leaders. That is a mental process that the strategic cyber campaign should be designed to achieve as effectively as possible.

Quantum Technology Implications: The implications for the cyber domain of future technologies that will employ quantum phenomenology are significant. These technologies may not have a major impact during the period of interest here, but it's still worth noting their potential. Nearest at hand and already available commercially is quantum key distribution. Further away from practical use are quantum computing, communications, and sensing. Quantum key distribution provides for highly secure encryption between cooperating entities. An attempt to acquire an encryption key transmitted this way is detectable and self-defeating. Quantum computing will provide a tool that will allow for much more efficient code breaking against many widely used forms of encryption, as well as other specialized applications. Quantum sensing and communications will provide enormous improvements in sensitivity, precision, and data transmission. It's impossible to predict when each of these applications will be available for general use; some are being experimented with at scale today and others are in early stages of development.

Reliability: Because cyber weapons are basically software, they can have classical software reliability or quality issues and can follow software reliability growth models. Cyber weapons tend to be single use expendable products. Once a cyber "projectile" is fired one can expect any opponent to react by quickly closing the metaphorical door the projectile flew through, so the same attack won't succeed again. Future cyber weapons will also operate on threat networks, where there is very limited opportunity, if any, to "burn in" the software and eliminate defects. Achieving high reliability, so the first and perhaps only field-use of a cyber weapon is successful is a design requirement and challenge.

Requirements Creep: This is less of a consideration in the Cyber domain than in others, but it still applies. Conscious attention should be placed on avoiding cost imposing marginal or low return on investment requirements.

[71] Much of the AI research in the commercial world has one purpose—to understand how to reliably manipulate people to buy offered products. The data the commercial world wants, and what ISPs and social media companies have, is the correlations between purchasing decisions and everything else about the consumer.

Resilience: The concept of resilience—the ability to absorb an attack, continue functioning, and/or recover quickly—applies much more to defensive measures than to offensive cyber weapons. The continuing evolution of commercial cybersecurity measures has largely incorporated this concept into existing IT system and application designs. I expect this to continue. Resilience for offensive systems is largely about the ability to avoid detection over time, both for access opportunities and for weapons, once a weapon has been implanted in a threat system host.

Responsive Threats: The cyber domain is aggressively two-sided and dynamic. Any new IT system or application will be probed for weaknesses immediately upon fielding, if not in development. Efforts to close any vulnerabilities will often be reactive rather than proactive, but they will also happen quickly. Early in the internet era, the advantage was very strongly with the sophisticated attacker. That hasn't changed, but the size of the gap seems to have diminished as defenses have improved. The commercial world has largely accepted some level of cyber threat risk because the economic incentives to do otherwise have been weak. Hardening critical national IT networks against the most sophisticated threats may improve in the future, but we can't expect to outpace the threat, especially the so called "advanced persistent threats" meaning nation states with well-funded, professional, and ongoing malicious cyber campaigns. Absent a breakthrough defensive technology event, which I don't foresee, we are just going to have to live in this world and design in as much hardness, redundancy, damage limitation, and graceful degradation capability as we can afford.

Single Points of Failure: Unfortunately, there are a lot of them, especially on the defensive side of the strategic cyber equation. Unless the government steps in and mandates designs that do not have single points of failure, we are likely to have them in our commercial infrastructure networks and systems. On the offensive side they are easier to avoid. Any future strategic offensive cyber campaign design should strive to have multiple ways to attack any given target and a redundant set of targets as well.

Sustainment: Once a strategic cyber suite of offensive weapons has been integrated into a campaign plan, there will need to be an ongoing activity to sustain the viability of that plan over time. This implies several actions. First, the suite of weapons must remain concealed. Some cyber weapons may be deployed in advance and hidden on enemy systems (something to be avoided, if possible, because of the risk of detection and exploitation), others may be deployed just before or at the outset of a campaign. In either case, the existence of the weapons and their means of access must be concealed over time. Next, the viability of any cyber weapon that is part of a strategic cyber campaign must be continuously assessed as threat changes through upgrades and defensive measure adjustments. Finally, new weapons have to be in development continuously as threat targets change with the introduction of new systems and capabilities.

Test and Evaluation: It's largely impractical to conduct either offensive or defensive strategic cyber domain testing at scale, given the potential scope of a strategic cyber campaign. As a result, we will have to rely on a mix of individual system tests, selective extensions of individual systems, simulation, and higher-level modeling. Some defensive testing at reasonable scale is possible, especially for acknowledged commercial products. Some defensive products may (should) not be

publicly acknowledged, however. Any offensive cyber weapon testing at scale would have to be conducted covertly. This is challenging and risky, but not impossible. Test programs will have to be developed to achieve adequate knowledge of offensive or defensive cyber system performance.

Training: During the Obama Administration we created a "cyber mission force" to substantially expand the size of the Defense Department's cyber human capital account. A lot of effort has been put into training those individuals. At this point I would expect we have a reasonably well-trained group of people to defend military networks and assistance in the defense of civil networks on an individual basis. I can't speak with any knowledge to our offensive capabilities. My guess is we have a long way to go in terms of preparing humans throughout the chain of command for their role in a large-scale defensive or offensive cyber operation of the type I imagine for the not-too-distant future. Before we can train people, we will need to develop the integrated C3BM system they would use and the suites of tools they would employ or deploy in a strategic cyber operation. The human machine interfaces associated with all of this should be developed in collaboration between those future cyber warriors and the software engineers developing the needed weapons and control systems; in many cases these may be the same individuals.

Other Needed Military Functions

Civil Support: A great deal of malicious activity in cyberspace is not military and does not involve nation state actors. The military and intelligence communities both have a role to play in assisting civil authorities to combat crime, malicious influence campaigns, and extremism and in supporting efforts to protect privacy and intellectual property. There is a tension between these goals and the role of the military and intelligence communities in U.S. society. My expectation is future threats will create pressure to overcome that tension for the common good. I can't predict how much that might change the defense establishment's role, but some support to these functions will be needed.

Electronic Warfare Support: There has been a lot of talk about the convergence of the EW and cyber areas. There is a relationship, but it is not particularly strong. Future strategic cyber concept designers should clearly consider all ways of accessing networks from both a defensive and an offensive perspective. Any RF portal can be a portal for EW applications or for cyber applications, at least in theory. In the commercial world one can jam or spoof wireless networks and systems like GPS as well as use cyber tools to protect or attack through these portals. Intelligence products of all types should also be shared without regard to the phenomenology involved in collection. Where it makes technical and operational sense, cyber and EW should be integrated, for both strategic and tactical warfare.

Intelligence and Counterintelligence: For a strategic cyber threat to be viable, the intelligence on which cyber weapons are based must be exquisite and constantly updated at a rate comparable to the rate at which changes occur in the target set. Some target sets may be fairly stable, while others will experience changes from periodic "patches" or security updates to complete technology refresh and system modernization. A lot of civilian infrastructure is old and infrequently changed, both in the U.S. and in the cases of potential opponents. A significant effort would have to be put into achieving and maintaining access, understanding threat networks, and keeping any implants

hidden and effective if activated. The counter-intelligence effort must include not just hardening against threats, but active programs to penetrate threats and stay a step ahead of their plans and operations. We already live in a world in which a shadow or gray zone struggle for intelligence and counterintelligence is being conducted. I expect this struggle to only increase in intensity as new technologies are fielded.

Psychological Warfare: The use of a strategic cyber threat as a deterrent or coercion tool is a form of psychological warfare. When implemented, a strategic cyberattack should be carefully structured to have the desired psychological as well as physical impact on the target leadership and/or population. Any collateral operations, be they psychological, kinetic, or non-lethal, should be structured and executed with strategic cyber operations to have the best collective impact possible. This all puts a premium on understanding the motivations, biases, and emotional pressure points of the intended targets, a very rich environment to apply some forms of AI. The ability to analyze and even experiment with human behavior through AI techniques will dramatically increase the potential for successful strategic cyber operations.

Special Operations: There can certainly be a strong connection between strategic cyber and special operations, but I would not assign the strategic cyber role to the special operations community. I would imagine a focused, dedicated effort with concomitant organizations as the appropriate way to organize for strategic cyber domain operations. I'm inclined to see special operations as having the same relationship to a strategic cyber operation that USSOCOM has to geographic regional commanders today. Special operations should be integrated into strategic cyber domain planning. Tactical use of cyber, on the other hand, should be integrated into more traditional special operations tactical planning.

Joint, Multi-Domain, and Combined Operations

Introduction

Joint, multi-domain, and combined operations have been around for a very long time. The synergies of integrating operations across Services, domains, and with allies are being emphasized now, and will continue for the foreseeable future. Advanced sensing, communications, computing, and integrated command and control technologies all provide opportunities to improve warfighting efficiency, both within and across domains and across organizational boundaries. The first modern iteration of this idea was "air-land battle" in the 1970s. In the 1990s, the label "network centric warfare" became popular. Today it is a combination of Multi-Domain Operations or MDO, and "Joint All Domain Command and Control" or JADC2, which has achieved almost a theological following among senior military leaders. The premise is technology has advanced to the point where integration and analysis of all sources of data, from all domains, into a timely decision-making process will confer a substantial advantage. My own view is there are advantages to be obtained by operationalizing command and control and AI-supported battle management technologies more effectively and broadly, but I think the hype may be overblown for three fundamental reasons: (1) specific payoffs from JADC2 have not been quantified or prioritized and may be less than expected, (2) the enemy gets a vote, and (3) the focus on ideal interconnectivity and information flow may cause overreach and failure and also may prevent the United States from pursuing more fundamental changes in operational concepts and systems that will have higher returns on investment.

With regard to overreach and failure, there have been ambitious attempts to merge information more fully in order to acquire operational advantage before. The Single Integrated Air Picture program undertaken by the Air Force was one. Another was the "Future Imagery Architecture" program to integrate space-based imagery. One I personally worked on was the Army's Future Combat Systems (FCS) program. All these efforts were ultimately canceled. I don't consider these failures to be dispositive about JADC2 or the idea that future forces will be much more integrated across domains—I think they will be more integrated—but I also think designing those architectures and investing thoughtfully in manageable increments with specific high payoff operational improvement is the right approach. Chasing undefined aspirational goals has made Joint C3BM the worst performing class of programs attempted by DOD.[72]

The first step needed is to address item (1) above and to determine what information moved where and integrated with what other information will be of greatest operational utility. Once that is accomplished the next step is to pursue that capability, assuming it is feasible, and to field a meaningful increment of improved performance. Here's where I would look for operational efficiency improvements. Firstly, in each domain we want to know where the enemy's most valuable assets are and what they are doing, and we want targeting quality data compatible with our delivery systems (launchers) and weapons (projectiles). Next, we want to make tactical and operational inferences or projections from that data to inform our own force distributions and

[72] See *Annual Report on the Performance of the Defense Acquisition System*, 2016.

movements and to plan and order coordinated strikes on the most important enemy assets, while simultaneously protecting our own forces and achieving favorable exchange ratios. All of this must happen as quickly and accurately as possible. Because we can't afford everything, and because some things are not even technically possible, it's extremely important to make good choices about how and where to invest. I'll offer some thoughts on this (subject to future analysis) shortly.

As one thinks about specific high priority payoffs, one also needs to consider the enemy's reactions. A unique feature of military versus commercial communications systems is someone is actively trying to shut military systems down, physically destroy them, or wrest control of them away. Given the peer competitors the Unites States faces, we have no alternative but to design for hostile jamming and cyber environments and to harden against or avoid targeting for physical attacks of various types. Our C3BM systems must be robust, both intra- and inter-domain.

With size and complexity can come vulnerability and complexity. Our multi-domain networks must be designed as scalable integrated robust wholes; a piecemeal approach is unlikely to be successful. One popular technique is to analyze "kill chains" (I'll credit my friend Paul Kaminski with coining this term of art) or high priority "operational threads." Both are useful approaches and good preliminary steps, but the so-called "minimum viable product" for JADC2 will have to be designed for maximum operational impact by enabling important kill chains or operational threads at scale ("one-of" engagements and "sniping" are interesting but not enough) and to be survivable or at least resilient with graceful degradation against all expected attacks. The key to joint and combine multi-domain operational efficiency will be timely and accurate management of complex many on many engagements using resources that cross both domain and functional spaces.

A lot of work currently is going into demonstrating individual threads of connectivity between systems that haven't traditionally talked to each other. This is fine, but it's an early baby step toward the much more difficult goal of integrated and highly automated operational battle management at scale.[75] I've seen too many cases of C3BM overreach that ended in failure. What I'm seeing now is an idealized vision on the one hand that may be over-promising, and uncoordinated specific demonstrations on the other hand that are not clearly tied to achieving a well-articulated or quantified operational benefit. Let's look at where those benefits might be most significant. I'd propose several integrated architectures, all of which I believe should be pursued incrementally and simultaneously, starting with the definition of a "minimum viable product" in each case.

Operational Concepts

If China has military ambitions with regard to Taiwan or any other offshore objectives in its near abroad, then surface ships are essential assets for pursuing those objectives. China's whole A2AD program is designed to prevent interference with China's actions close to its own shores. Surface ships are relatively targetable, and the target speeds provide opportunities for engagement with over the horizon launched weapons from air, land, sea surface, and sea sub-surface launchers. While space-based sensors would be part of this concept, both air and sea-surface, and potentially

sea-subsurface sensors could also be employed and integrated. The projectiles (anti-ship missiles of various types primarily) will be most effective if times of arrival, target deconfliction, and tactics are coordinated, independent of the launch source of the weapon. One can imagine this operational architecture being built up over time from the most cost-effective building blocks. A key element of this version of multi-domain operations would be the full integration and inclusion of regional allies with their own land, air, and sea-based weapon systems and ISR systems.

> Integration of the systems that could defeat an aggressive land movement intended to seize terrain in Europe, most likely of a NATO ally: Space, air, and perhaps unattended ground sensors would provide enemy force movement and operational intent information and support targeting, primarily for weapon delivery from air and ground-based launchers. This concept is a direct descendant of the "Follow-on-Forces Attack (FOFA) systems developed in the 1980s as a result of DARPA's Assault Breaker project. A modern version would integrate space-based systems as well as unmanned aircraft (both as sensor and weapon transporter/launchers) and autonomous ground vehicles.[73] It would also be essential to integrate NATO allies into this concept and to coordinate fires from all sources for maximum impact.
>
> Integration of defensive counter-air and ground or sea-based air defense systems into a single multi-domain C3 system: Again, space-based ISR plays a critical role, but timelines are much shorter than for ground or sea surface targets, and automation will be necessary to respond effectively to threat attacks at scale. This isn't really new conceptually, but I don't think we've ever solved this problem for cases that involve large numbers of coordinated attackers. This construct has value in both the Asian and European scenarios. As a former Army Air Defense officer who served in the Hawk Belt in Germany under the Command of the Fourth Allied Tactical Air Force, and someone who was closely involved in the First Gulf War and the attempt to glean lessons learned from that experience, I can say with some confidence that integrating air defense and friendly air operations isn't easy. When the threat includes cruise and ballistic missiles, as well as enemy aircraft (manned or unmanned) and intense enemy jamming—this is a "wicked" problem. It isn't an intractable problem but solving it at scale will mean a reliance on automation and decision making with imperfect data as well as close integration with allies. NATO has labored for decades to develop an integrated air defense command and control system with only marginal progress to show for it. An incremental approach is certainly called for here. One helpful feature of the air domain construct I described above is that the willingness to accept some degree of attrition of unmanned systems by friendly fire should make this problem much easier. There is a high, even insurmountable barrier in the U.S. for the idea some losses of Air Force pilots to friendly fire from ground-based air defenses might be

[73] When I was DDR&E for Tactical Warfare Programs in the late 80s and early 90s the FOFA basket of programs reported to me as a separate high priority office. The looming potential for the FOFA programs to checkmate a Soviet mechanized invasion of Western Europe may have been a factor in the attempts at reform and the ultimate breakup of the Soviet Union. FOFA programs were at the heart of the dramatic victory in Desert Storm, which in turn was a major motivator for the Chinese A2AD suite of programs.

acceptable—it is not. For areas in which only unmanned systems are operating, there should be much more flexibility.[74]

Integrated space control and space control related operations focused on controlling and dominating the space domain: Space control campaigns must be designed to both protect U.S. assets and defeat enemy counter-space and space systems across multiple domains. The fight for control of space is likely to be determinative in a future conflict, but it isn't just about the space domain itself. It must include the kinetic and non-kinetic targeting of ground-based C3BM of space offensive and defensive systems themselves and of efforts to protect the ground or sea-based space control and surveillance systems and space launch systems. The high premium for being the "first actor" or to achieve surprise in space dictates that space-focused joint and combined operations be operationally ready to respond on short notice (minutes or even seconds) to hostile acts and across multiple domains.

Building Blocks

While C3BM systems to support joint and combined operations will each have some unique features because of the physical characteristics of the domains and operational constructs involved, there is also a "common core" operational technical architecture, at least conceptually, that can be applied in each of the cases described above and in other cases. There is a similar "generic" problem at the heart of each of the various multi-domain problems. One can think of this as a meta-C3BM system that functionally integrates data from specific sources, especially targeting data, and processes it to provide optimized targeting assignments and an efficient allocation of resources together with plans to employ those resources. In each case, this common core meta-system must have the capacity for continuous updates, some degree of tailorable human oversight, and high degrees of automation that produce reliable, timely results. Another feature of this meta-C3BM system will be its scalability, so it can be employed as the operational C3BM kernel at various operational levels. One approach would be a core set of capabilities with APIs that specify formats for inputs on sensor data, weapons characteristics, force deployment and employment guidance, and other factors.

A critical design feature for any implementation of the common core I've described is the number and type of assets that can practically be integrated into the "minimum viable product" for the specific Joint Multi-domain instantiation. Each of the several examples I provided for Joint Multi-domain operations will have its own "sweet spot" at some level of force integration where technology and operational utility intersect. One immediate goal should be to define what level of integration that represents and to break down the barriers to achieving it. We can then design

[74] In the U.S., this wicked problem is compounded by the fact that the Missile Defense Agency (MDA) is only directly responsible for ballistic missile defense—which excludes cruise missiles and aircraft. During my tenure as USD (AT&L) I assigned MDA with the role of chief systems engineer for integrated air and missile defense, but my sense is that this was not seriously implemented due to Service reluctance to accept any outside direction that might have imposed costs.

operational implantation around groups of capability, each of which is sized at that level of Joint Multi-domain integration. Our organizational structures, where we are likely to put human executive control functions, should reflect that same level of operational integration.

While the description of this building block may sound straightforward, it is anything but.[75] The most unsuccessful programs in DOD history are Joint C3BM programs.[76] There are probably several reasons for this, but the most important two may be these systems are very hard to design, and they require sound timely decisions involving compromises among the joint participants to move forward. I believe the technology exists now to effect the type of system I have described, and it will only get better over time. The harder problems, for the U.S. at least, are getting the parties involved to cooperate, getting timely technically-sound decisions on the needed specific design features, and achieving cross Service and organizational implementation of those decisions.

Complexities

Fundamental Operational Needs

Multi-domain Asset Management: If we want to be able to fight in various contexts using truly multi-domain forces, then we have to think of force or asset management as a multi-domain and multi-Service problem. Current joint forces are organized from below the Joint Task Force (nominally a multi-wing, multi-brigade, and possibly multiple carrier strike group size force) level on down by Service Component commands. "Jointness" tends to stop at a high operational level. In the various domain and multi-domain concepts I've described, there is generally a tactical level point at which I've placed humans who are controlling operations of what can generally be thought of as a single Service force, but with inputs and dependencies on multi-domain assets—especially space assets. If multi-domain operations are to be a reality, there must be a capacity to manage cross service assets efficiently and operationally responsively to support multi-domain and domain specific operations with multi-domain dependencies. I don't think this should happen at the tactical echelon I describe in each concept. It may happen one layer up, but in many contexts, it may be two layers up. The assets of concern are not just DOD assets, they also include intelligence community assets and allied or partner assets. I don't think there is a technical barrier here that is insurmountable, but the U.S. has never been good at this and in many cases has defaulted to single Service solutions and creative expedients. In wartime, motivated leaders find work-around ways to do their jobs as well as they can, often with human intensive brute force methods. We will not have an effective multi-domain force in the future unless we solve this problem, which like other barriers is more about culture and leadership than it is about technology.[77]

---

[75] I can picture a block diagram of the core C3BM concept that looks roughly the same for each operational context. ISR information flows in decisions are made with human oversight and orders to force echelons flow out. There is a feedback loop from operational forces and continuous ISR input and episodic order generation. Within the controlled tactical force there are automated integrated behaviors.

[76] See *Performance of the Defense Acquisition System,* 2016.

[77] The C-JADC2 effort is intended to address this issue, but so far, I haven't seen much substance to support the rhetoric.

Command, Control, Communications, and Battle Management: C3BM is the brain and nervous system for joint and combined multi-domain operations. I discussed the common core idea for tactical force management earlier and the integrated multi-Service, multi-domain asset management function at roughly the operational level above. In the future, we will also require an integrated and hardened multi-echelon C3BM system to control and support forces at all levels. While we can and should use cutting edge commercial technologies in this system, I don't think those technologies will meet military needs unless the DOD makes significant investments in adding security and resilience for our military systems. Ideally, DOD should be a step or two ahead of the commercial products for performance as well, but given the amounts being invested in the commercial world that may not be possible.

Planning and Rehearsal: This is an embedded function in the C3BM system, but it's worth thinking about independently. Classic planning happens simultaneously on different time horizons—call them short-, mid-, and long term. The differences traditionally are measured in days, at least at the operational level of force management. The future planning process should be much more dynamic, situation-dependent, responsive, and continuous. It should also be much more automated. Rehearsal will be embedded in the planning process as part of planning and course of action analysis at the level where humans will be engaged and interacting. Both planning and rehearsal should be through sophisticated simulation and with accelerated time. I envision the future force efficiencies that will allow us to dominate on a future battlefield will occur at two levels. The first level is the highly automated tactical engagement level with multiple platforms engaged against multiple platforms using automated behaviors and engagement decisions. The second level is here, at the echelon in the joint or combined fight where humans exercise executive decision-making supervision over multi-domain operational planning.

Logistical Support: If we are going to be successful against great power opponents with any future operational concepts, we must have a secure and operationally resilient logistics system. While the number of people in the force concepts I've described is greatly reduced, there are still plenty of humans in the concepts and they will have to be logistically supported with food, medical care, etc. Consumables must be provided including fuel in some form and munitions. In many cases forward maintenance is reduced, and some attrition of unmanned systems is expected, but there will still be maintenance and extraction requirements as well as mobility support requirements for a wide variety of needs. Automation, ubiquitous sensing, and advanced data analytics will play major roles in improving the efficiency of future logistics support systems. These technologies can be developed and integrated at a pace driven largely by civilian investments. What concerns me is the reluctance to appreciate the extent to which these systems are targets for both cyber and kinetic attack by our adversaries. If we don't design and harden our logistics systems for the likely threats, then we are creating a very visible Achilles heel for our future force.

Mission Variations: A joint or combined force could be called upon to do almost anything. The U.S. military provides a massive set of tools that is usually not involved in major conflicts and available to support the nation as needed. The list in my memory includes humanitarian relief in a natural disaster, establishing a blockade, assisting in responding to a pandemic, conducting a hostage rescue, eliminating chemical munitions at sea, raiding a terrorist hideout, rebuilding or

building a less developed nation's military, responding to cyberattacks, enforcing no-fly zones, counter-proliferation, peacekeeping, and counter-piracy. I'll briefly discuss these and others below. There are also a range of tactical missions normally associated with military conflict and force: counterinsurgency, raids, covert operations, limited air campaigns, etc. All the forces I've described were conceived as ways to become more efficient in a conflict with a peer or near-peer competitor, but while that may be the most important capability we want, it certainly isn't the only one. Any future force design will have to take into account the full range of mission variations the total force should be able to perform. This will undoubtedly lead to some specialized units and equipment, and in many cases to more human intensive organizations than the ones I've described. My view would be to start by assessing the capabilities of the concepts I've described to deal with the range of possible missions. The assessment should focus on the adequacy of the joint and combined multi-domain C3BM structure and logistics structures. Once that exercise is complete the need for specialized units, people, and equipment can be determined and prioritized.

Design Requirements and Considerations

Anti-Tamper: We will have to assume that almost any, but especially the forward echelon C3BM nodes, will fall into enemy hands and be reverse engineered. We will also have to ensure commercial products utilized by DOD securely protect sensitive information, even if they fall into enemy hands.

Civilian Engagement and Interaction: All our forward deployed Joint multi-domain forces will have to interact with local civilians and likely with civil authorities. Some of these interactions can be accomplished or navigated by autonomous systems or through remote virtual contact, but many will demand some degree of established trust and intuitive decision making that only humans will be capable of for some time into the future. Automated translation devices, for both audio and print, should make these interactions more productive and efficient.

Collateral Damage Avoidance: As in the individual domains, joint and coalition multi-domain forces will need to manage collateral damage avoidance consistently with the laws of war and hopefully with far fewer errors than in recent history. C3BM systems and target detection systems will have to meet established thresholds for false positives and include a continuous machine learning feedback loop to improve their performance. Effective human supervision must be provided over a range of situations and operational tempos. That cannot mean every engagement has to be approved once conflict at scale is initiated, but the C3BM system must provide for meaningful and effective control and supervision over a full range of situations.

Confidence in Automated Behaviors: As one moves up in chain of command levels or echelons and increases the reliance on off-board cross domain sensing, C3BM, and fires, the complexity and the potential for unforeseen errors increases. Within this more complex context it is harder to anchor confidence in extensive field testing or operational experience, making it important to collect as much data as possible from live training or actual conflict and to integrate that data into modeling and simulation designed to boost confidence in automated behaviors at scale. I would expect any future suite of interacting systems involved in multi-domain operations would be

subject to continuing confidence building analysis and human oversight in a machine learning, continuous improvement environment.

Counterintelligence: As both the U.S. and its peer or near-peer adversaries move towards greater reliance on autonomy and connected architectures, the value of intelligence, and therefore, of effective counter-intelligence increases. Joint and combined C3BM systems and the people who design, build, and operate them will be high priority intelligence targets. We Americans are not adequately attuned to the degree to which our systems, and we as individuals, are targets of intelligence collection. Some forms of AI will give us opportunities to be more proactive in our own counter-intelligence activities, but we will have to do so within the legal constraints placed on searches in the U.S.

Countermeasures: At this point, I don't see any obvious opportunities or needs for specific cross domain countermeasures against current classes of weapon systems. The types of countermeasures noted earlier in each domain are generally self-protection systems. Designers of future cross domain concepts should be thinking about integrated resiliency. As an example, one possibility might be a ground-based air and missile defense system with an increment of capability to defeat a low earth orbit co-orbital ASAT.

Cultural Resistance: This may, in fact, be our biggest impediment to achieving Joint and combined multi-domain systems and concepts of operation. It used to be Air Force written doctrine that "only an airman knows how to employ air power." It probably still is. The other services have equally strong views, whether they are written doctrine or not. There are valid reasons for a degree of protectiveness over Service prerogatives and roles, but those attitudes also serve as barriers to improvement the U.S. cannot afford in a great power peer or near-peer contest. My own view is the U.S. needs a cadre of people who are truly Joint, and only Joint. This is a controversial subject and provokes a lot of anti-bodies, but we can't expect officers whose careers will essentially always be controlled by senior officers of one Service to ever look very far beyond that Service's vested interests.

Cyber and EW: With the partial exception of the undersea domain, neither cyber nor EW will respect any spatial boundaries, and any radio frequency or even optical aperture can conceivably be exploited for both. As stated earlier, I feel the convergence of cyber and EW is not as great as others might believe. Nevertheless, the RF world is increasingly software-defined (meaning that functionality once performed by analog devices is now digital) making cyber a lucrative way to affect signals and signals a potential way to insert malicious digital content.[78] In the multi-domain world, cross domain cyber and EW hardening, and attack options must be considered and included in all designs.

Deception: As mentioned earlier, deception is under-rated and underutilized in the U.S. It can be a huge force multiplier, especially at higher Joint and Combined echelons. It can also be a major

[78] Software defined up to the point at which RF signals are transmitted or received. Digital representations of signals and waveforms still have to be converted to radio frequency energy to be transmitted and from radio frequency energy into digital representations after they are received.

contributor to deterrence, although relying on bluffs about nonexistent capability is a very dangerous tactic, and an even more dangerous strategy. Deception should be a serious and conscious decision at the joint and combined levels and as investments in future multi-domain capabilities are analyzed and compared. Doing this well is tricky because of the tension between deterrence and operational capability; convincing an enemy we are weak where we are strong would weaken deterrence, but the perceived potential to have concealed capability where we appear weak could strengthen deterrence. The simple formula to render deception unnecessary is to be strong everywhere and make sure the enemy knows that. The U.S. may try to be strong everywhere, but it isn't clear we can afford or achieve strength in all domains or in all combinations. The next best option is to appear strong everywhere and be strong where it's the highest payoff for the investment. We also may want to appear weak where we are strong in order to convince an adversary to invest elsewhere, or to make investments we can easily defeat. One can go on with this convoluted logic for a long time, but the default to not attempt deception at scale could forego high payoff options for both deterrence and operationally. Active deception programs are possible in all domains, but cyber, space, and undersea—because it's relatively easy to conceal capability in these domains—offer some interesting potential.

Default Behaviors—Loss of Contact/Control by Echelon: As we move up in scale to cross domain Joint and Combined operations, the implications of loss of control over elements of the force or of classes of capability (think total loss of space-based ISR for example) become even more significant. This argues for some degree of redundancy across the board. We should not make a major part of the total force completely dependent on a capability that might be eliminated or disconnected by enemy action. I've generally posited a future force that depends on functionality from space in every other domain. There would have to be some degree of degraded backup capacity for all the support functions provided from space. Structural resiliency and default behaviors for when supervision or external support are lost should also be designed into the architecture.

Energy: The energy needs of the entire Joint and Combined multi-domain force should be considered as a whole as part of the design process, not just for each domain or platform type. The current force consumes vast amounts of petroleum-based fuels for mobility and supporting organization operations. Fuel has been a limiting factor operationally on many occasions. It will be even more so when large, fixed distribution and storage systems are susceptible to attack by a sophisticated peer competitor. I do foresee more efficient energy sources becoming available, but I don't foresee a way to eliminate having a substantial logistics support tail for stored energy and the necessity to distribute energy in some form to the operational force.

Humans—Location, Role of, and Support To: If we are going to fight in an integrated multi-domain way in the future, we will have to redesign our command-and-control organizations. For example, instead of an Air Operations Center (AOC), we might need an Air/Land/Space Operations Center. That ALSOC would also include strong cyber and EW elements. As noted above, I would envision this type of headquarters being one or perhaps two echelons above the domain specific C3BM nodes where human executive supervision of single domain-centric operations occurs. The location, size, and capabilities of these multi-domain C3BM nodes would

be tailored depending on the total force assigned and the mission context—form follows function. I can foresee a cadre of operators with a very special set of skills working in these units. Automated data analytics, decision support tools, course of action generation and analysis would be utilized and continuously upgraded through machine learning and feedback. These nodes would have to be logistically supported, secure, and redundant. They could conceivably be distributed or disaggregated and connected virtually. See the discussion of Organizational Structures and Training below for more on this topic.

Identification Friend or Foe (IFF): It would be desirable to have a universal "Blue Force Tracker" for all platforms in the entire Joint and Combined Force—across all domains and including allies. It wouldn't have to be an interrogation and response system like classical IFF, but it would have to be reliable and precise. The maritime AIS system offers an analogy as do the traffic monitoring apps we all have on our cell phones and the RF tags for tracking commercial containers or packages in transit. I offer as a hypothesis that technology can support this requirement and do so in a contested environment in a way that doesn't compromise friendly asset locations to an enemy. Having a system like this would pay fratricide avoidance benefits, but it would also be a source of exquisite friendly force situation awareness and support operational and logistics planning. As an initial design goal, I'd suggest starting with a combined air and land domain capability that could be used to support friendly force situation awareness and control as well as individual autonomous engagement decisions. As in other areas, the biggest obstacle to fielding something like this across the Services may be cultural, not technical.

Information Management: At the joint and combined multi-domain level it is hard for me to conceive that real life technical limits won't constrain data processing and analysis functionality. As exciting as new data storage, communications, and processing may be, they won't be infinite. Future military information architectures will have to be designed around real-life constraints, and as I've noted elsewhere, I think there will be a need to keep the bulk of the data storage and data processing near the operational edge of the networks. We will also need to design for graceful degradation as information network nodes are attacked or severed from the network. Commercial cloud architectures are the current rage, and with good reason, but their resilience in a wartime setting must be taken into account in a future multi-domain construct. Optimal data management architectures change every decade or so as technology advances unevenly across the relevant functions. The commercial world will drive this; the military must stay poised to be a fast follower and integrate military requirements into emerging new information management concepts.

Intelligence Fusion: Future joint and combined operational concepts have to include powerful data fusion engines that operationalize disparate intelligence data sources across domains. The design challenges are significant, but not insurmountable. However, two non-technical obstacles will have to be overcome. First, the operational and intelligence communities will have to merge—there can't be a sequential intelligence analysis function before intelligence is integrated into operational planning. Second, the Services and Intelligence Agencies will have to come together on a single integrated multi-domain information architecture in which all source intelligence can be fused. Neither of these tasks will be easy, but both are essential if we hope to integrate intelligence into operations effectively.

Interoperability: Most aspects of interoperability within the U.S. structure (cross-Service information management, intelligence fusion, etc.) have been discussed under other topics. If we are going to integrate our allies and partners into multi-domain Joint and Combined operations, we will have to proactively determine where the highest payoff opportunities exist and work to realize them. I'd suggest full or nearly full interoperability is possible with some traditionally close allies, but in other cases we will want to be more selective. In terms of payoff, getting real time or near real time access to allied and threat dispositions and targeting quality threat track data so that the U.S. could include those targets and allied assets in its operational planning and dynamic retargeting would be high on the list. This is true across domains.

Legal Constraints: Laws of war apply even more at this level and may be harder to implement. Processes that satisfy these constraints must be included in the cross-domain architecture. There will be many cases where engaging launchers or projectiles and even highly automated units may not have first-hand data on target ID, especially for beyond line-of-sight engagements, which one hopes would be the norm. The criteria for approving these engagements must satisfy international law norms against indiscriminate collateral engagement, attacks on protected humanitarian and cultural sites, etc. In addition, at this level constraints like overflight rights, encroachment on neutral territory, etc. must be included in operational planning. Planners have to take all the relevant constraints into account today. Future systems should provide even more effective and highly automated ways to impose the required constraints.

Operational Planning and Rehearsal: Linking Joint and Combined multi-domain C3BM to enable planning and rehearsal at whatever scale is needed is analogous to the movement in engineering to Model Based Systems Engineering (MBSE) which links models across the design stovepipes and across development, production, and sustainment. Under an MBSE construct many design configurations can be digitally defined and tested through simulation. This is a currently still an emerging capability, but the trend is clear, and it applies in the operational world as well. The JADC2 and various Service counterparts are intended to provide both operational execution and planning capabilities. There is an enormous amount of work to be done to make this real, but it has started, and I don't see a technical showstopper. I do foresee issues with cultural stovepipes, reluctance to accept the cost to change to accommodate integration with others, and difficulties with integrating even close allied partners. All this argues for beginning with one or two high payoff use cases (at scale) to improve the chances of success and to provide a meaningful increment of capability as a starting point.[79]

Organizational Structures: Current organizational structures are too rigid and too single Service. As noted above, for a major operation a Joint Task Force is normally formed today with Service Components as the major organizational elements. Within the component organization one finds traditional structures like wings and brigade combat teams, which are certainly tailorable and can be augmented, but which are still essentially single Service. To get the full benefit of cross domain operations in the future, we will need more tailored and mixed operational structures that are

[79] The recently approved JADC2 Strategy document lacks specific mission applications or operational goals. In my view, any plan to implement the strategy should be focused on achieving specific operational results.

designed around coordinated actions to achieve specific operational missions. As a starting point, we should consider future structures where every echelon above the basic tactical fighting unit is joint and involves the integration of operations in multiple domains. A space, air, land construct and a space, air, and sea-surface construct would be two reasonable starting points. At the other end of the spectrum—total force capabilities—the U.S. should also consider a "Global Operations Command" that provides multi-domain resources and support functions to all geographically regional warfighting commands.[80]

Physical Security: Joint and Combined multi-domain organizations for operations of any significant size will be complex networks with important command and control, transportation, and logistics nodes. A thinking adversary will be looking for weaknesses and points to attack, by any means that will have the largest impact on the force's ability to function. Concealment and deception can play a role in avoiding some attacks, but there will also be a need to physically protect against a range of threats, including special operations, covert operations and sabotage. Unmanned security systems and barriers can play a useful role in providing physical security, but complex situations and innovative threats can occur, driving an enduring need for human controlled and managed responses to the full range of possible threats.

Reliability: The networks that support joint and combined multi-domain operations must be reliable to function over time and under stress. Redundancy and graceful degradation should be designed into C3 networks, for all types of attacks. Classical reliability—the length of time between equipment failures while in use—has to be adequate enough to ensure operations will not be degraded due to reliability problems. Commercial electronics should be adequate to support much of this requirement, if they can also meet all needed military requirements including secure and trusted supply chains. Software and data systems that enable C3BM must also be reliable under operational stress, including under cyber and EW attack.

Requirements Creep: I'll play this record one last time. Conscious attention should be placed on avoiding cost imposing marginal or low return on investment requirements. The natural tendency in all domains, and especially in committee-designed multi-domain applications, is to add more and more requirements to the design until the concept crashes from its own weight. A lot of the items on this list are good examples of potential requirements creep. The whole point of the concept is improved cost exchange ratios over current systems.

Responsive Threats: I would expect the first line of response would be to try to identify and attempt to destroy critical Joint and Combined C3BM nodes, at each echelon. I would also expect attempts to emulate the capability described here, beginning with appliques to current organizations. The U.S. has already been very public about its intent to rely on MDO. I'm sure potential adversaries

[80] This is probably a whole other paper, but the basic idea is the U.S. could use its global interior lines to organize some assets on a global basis operationally. This would include space assets, transportation and logistics assets, some cyber assets, some airborne ISR and EW assets, global strike assets, and needed C3BM. For a great power conflict, or even a regional one, this command could "swing either way" in support of operations in Asia or Europe for example, as needed. It could be either the supporting or supported command depending on the situation. The U.S. provides Joint global services now, but in a piecemeal way from multiple organizations.

are already working hard collecting intelligence and analyzing how best to defeat any important U.S. advantages that materialize and on how to field a superior version before the U.S. fields its systems. Some existing threat systems, such as long-range surface attack conventional missiles or anti-satellite systems, could be easily adapted to target Joint C3 nodes.

Single Points of Failure: It I had to pick one of concern now, it would be Precision, Navigation and Timing systems—especially GPS. All the ability to fuse target tracks, merge identification data, develop common operating pictures, conduct adaptive EW, enable cognitive sensors, and plan complex multi-domain engagements or operations depend on reliable position and timing information, currently supplied chiefly by GPS. Some surveillance systems, like AWACS and Joint Stars today, can effectively be single points of failure. A future force must expect any single friendly asset or small group of assets can be identified, attacked and destroyed—if the adversary is prepared to pay the price of achieving that goal. An integrated multi-domain force has to be designed to deny that opportunity.

Stovepipes: The DOD is currently designed around stove pipes of operational expertise, which in turn have their own communities of people who share training, unit assignments, and career paths with each other. Generally, these stovepipes are associated with certain classes of equipment (surface ships, artillery, jet fighters for example). None of these communities are inherently joint or combined or multi-domain. All of them have their own cultures and are both proud and protective of their operational roles. Future forces, and the people who command them, will have to break this paradigm to be successful. As we move toward greater reliance on human executive control of operations conducted largely by formations of autonomous unmanned systems operating in a multi-domain environment, we should also create operators who are inherently multi-domain and who become skilled at Joint and Combined operations early in their careers.

Sustainment: Managing the sustainment of a Joint multi-domain force that is highly dependent on autonomous unmanned systems will bring a set of unique challenges, not the least of which will be avoiding providing an adversary with high payoff vulnerable targets. One risk that will have to be addressed is the potential dependency on cloud processing and data storage and the possibility that cloud infrastructure may provide “cheap kills” for an adversary, by direct attack or by attacking dependencies like the power distribution system. The entire supply chain will have to be resilient and structured with threats in mind. Special attention will have to be paid to having war time consumables including munitions and high demand spare parts and survivable transportation to get these and other items where they are needed. One should expect the range of possible attacks from cyber to long-range kinetic precision weapons to sabotage to be employed.

Test and Evaluation: Testing at scale, and testing against likely responsive threats will be challenging, but both are absolutely necessary. A lot can be accomplished with linked virtual human operated C3BM nodes and a mix of real and simulated platforms and autonomous platforms and units, but there has to be a realistic set of data based on field data to anchor the virtual simulation world. The test, evaluation, training, and rehearsal worlds all have a lot in common, but there must be adequate resources to meet each need.

Track Fusion: This challenging problem is at the heart of realizing battlefield efficiencies from multi-domain integration. It enables the efficient allocation and coordination of strike forces and precision weapons. History suggests strongly this capability should be developed incrementally, starting with the highest payoff use cases and growing from there. Single platform fusion of multiple sensors should come first, followed by integration of those tracks with the highest payoff independent multi-domain sensors. The technical issue isn't making multiple sensors for a single threat track to merge, but correctly sorting out for weapon allocation many tracks in a confused and cluttered many-on-many battlespace against an enemy that is doing its best to confuse us.

Training, Experimentation: A new class of Joint operations military professionals, of all grades, will be needed to achieve the future multi-domain concept I've described. They won't be developed and trained in the existing Service specific professional military education systems. They will fight intensely, but from screens that control multi-domain forces. They will need to train close to continuously. They won't be adequately trained through infrequent exercises in which threats are curtailed to provide a more benign operating environment so all exercise goals can be met, something that is the historical norm, especially for problems like Jamming and cyber threats.

Other Needed Joint and Combined Military Functions

Air and Missile Defense: This function was described in the air domain section and also the sea surface section, but it is a concern in all domains and a major reason for linking domains together. Future space sensors must provide early warning and tracking adequate to hand over threats to other air and ground-based sensors, if not directly to weapon (projectile) seekers. Air and missile defense requirements cover the tactical, regional, and intercontinental threats and the range of ballistic and cruise missiles and aircraft including hypersonic weapons. They also include warning and indications information and analysis and support to strike against ground targets including mobile launchers. All of this functionality, including that required for strategic (nuclear) defense, should be designed together to provide a balanced suite of multi-domain capabilities.

Air lift and Sea Lift—Strategic and Tactical: The forces I've described have transportation needs of various types, but much less than current forces. Some forces can self-deploy, but all will need sustainment support. I haven't tried to size the dedicated military lift assets that would be required. A lot depends on the degree to which prepositioning is used to reduce deployment time. Given emerging and future threats, I would support keeping as much material forward as possible. As noted earlier in the paper, ground combat units at scale, even with the lighter vehicles and reduced ground support fleet of trucks, must come predominantly by sea. The mass and volume are too great to do otherwise. This makes the large ground force deployment lead time weeks instead of days or hours. By relying largely on UGVs and small UAVs for the ground domain, it is relatively easy from the personnel management perspective at least, to preposition ground domain equipment forward, reducing the need for sea lift. The low numbers of humans in those forces also reduces the need for air lift of passengers. For both types of lift, unmanned systems are a possibility, but using manned systems does not impose a heavy penalty. As forces are sized for the relevant operational plans, air and sea lift can be sized to support those forces and plans.

Chemical and Biological Warfare: As chemical and biological threats are used largely to kill or incapacitate humans, the reduction in humans in the forces I've described should reduce the incentive to acquire and use these weapons. Nevertheless, they could still be used against specific targets and any place where humans have to live and work will have to be protected. Most chemical and biological detection systems today require close proximity and physical sampling. If practical airborne sensors can be developed, that would be a valuable capability. In any event, the multi-domain C3BM system will need the ability to efficiently integrate chemical and biological warfare related information and to use AI based tools to analyze that data and recommend actions.

Close Air Support: I've always been a big proponent of this capability as it is an important enabler for troops in contact on the ground. With the combination of the reduction in humans involved in line-of-sight combat and the availability of large numbers of small lethal UAVs, it isn't as significant for the air domain forces to provide support to troops in contact. As a result, air power can be allocated with a higher net effectivity. That said, there is no reason why the envisioned air domain assets couldn't provide this function when asked to do so. It should be an inherent capability of the multi-domain force.

Combat Rescue: This probably should be thought of more as emergency extraction, as there should be few cases of aircrews forced down behind enemy lines. I envision a small fleet of unmanned vertical lift air vehicles that would be used in certain situations to extract people, and possibly also insert or extract equipment, in hostile territory. This could be common with the tactical vertical lift capability described in the land domain section, but with more survivability features.

Counterterrorism: In my view, counterterrorism is not fundamentally a military problem; it's more about law enforcement and public physical security. The future military will continue to play an important supporting role when force needs to be applied. Most military counterterrorism operations would be conducted by Joint and Combined special operations elements. There is a logical extension of the extensive capabilities to conduct these sorts of operations (surgical strike, hostage rescue, raids, seizures, interdiction, etc.) that were developed after 9/11 but with the future integration of emerging advanced technologies. These operations inherently blend elements from multiple domains and are often conducted with friendly non-U.S. forces. They also involve intelligence and law enforcement personnel from outside the defense establishment. Humans will continue to have major roles in these missions because of their complexity. New tools should be available to support these missions from a range of technologies. One aspect of counterterrorism that may advance dramatically is information operations, which may not be a military operation per se but could well be decisive at addressing root causes and the ability of terrorist groups to recruit and grow.

Counterinsurgency: It's possible the U.S. could be drawn into another direct military role in a counterinsurgency campaign. This would certainly be a land operation with strong air, space, and cyber domain elements. Like counterterrorism, the U.S. military should be in a supporting role for other elements of power and local military forces, but there would be a stronger military element. The use of unmanned systems would permit more restrictive rules of engagement (up to a point), something that would be beneficial to the goals of a future counterinsurgency campaign. In a

persistent counterinsurgency situation, I would expect the ad hoc application of emerging technology to the situation's specific and unique characteristics, but hopefully with less lead time than in the U.S.' recent experience.

Disaster Relief and Humanitarian Assistance: The multi-domain capabilities of the U.S. military will continue to be called upon to support this mission. These include space and airborne surveillance and situation awareness, emergency logistical support, medical support, engineering support, and evacuation. This won't be a major driver on force design or equipping, but there will still be applications of military capabilities to this mission. Some of the capabilities of the mulita-domain forces I have described will enhance the ability to perform this mission.

Gray Area Influence Operations: Included under this rubric are information operations, sabotage, para-military operations, and population intimidation in various forms. The U.S. military may be asked by an international partner to assist in the defense against these types of operations. The U.S. should have the capacity to bring integrated multi-domain capabilities to the table, but I don't see this mission as a major driver of force design or equipment choices in general. A combination of this mission, counterterrorism, and counterinsurgency could lead to the inclusion of some specialized multi-domain units in the total force.

Medical or Noncombatant Evacuation: There will be some inherent capacity to provide this support function by air, land and sea. Because the future Joint force will be much less human intense, it may not be close to the scale of capacity the current force has. There simply won't be the need for military purposes.

Mine Warfare: The multi-domain aspects of mine warfare largely involve use of multi-domain sensing to facilitate effective mine deployments, detection of mine emplacement activities, and support to operational mine clearance. Cross domain requirements for sensors and information processing systems should include mine warfare related needs and opportunities.

Pandemic Support: This is not a core mission for the Joint force and won't be, but the inherent capabilities of the military can be used to support this mission. As with medical evacuation, the force will have a much lower need for medical capacity relative to the current dense human force, so the inherent capacity may be much less than currently.

Special Operations: Some SOF missions have been addressed above under the counterterrorism, gray zone, and counterinsurgency topics and/or in the other domain specific sections. The U.S. will continue to need a suite of multi-domain special operations capabilities and specialized units, for use in any type of mission, and this is likely to remain a human centric capability with autonomy and specific forms of artificial intelligence applied to various aspects of the mission over time as technology matures.

Training and Assistance Missions: The Joint force will still be asked to perform these missions, but its capacity to provide that support may be greatly reduced with the shift to unmanned systems. As our allies move in the same direction, there will be a need to train together for Combined and Joint operations using multi-domain capabilities. The ability to train less-developed nations with more traditional conventional forces will be curtailed relative to current capacity.

Conclusions and Closing Comments

Warfare has a logic of its own. When new technologies emerge that enable more effective military forces, those technologies will be adopted to that purpose. Sometimes new technologies affect the established identity of a "warrior class" whose existence and status is tied to the application of older technologies. When specific warfighting roles and identities are threatened, change can be resisted fiercely. But the change comes anyway. Military professionals whose status depends on their roles and which have been successful in the past are the most inclined to resist change.[81] In addition, success does not breed operational innovation. The conventional wisdom is Germany's defeat in WW I led to the development of the blitzkrieg operational concept, even though other countries had similar or superior technology. The U.S. has had extraordinary success in conventional operations since the end of the Cold War, at least against nation state militaries. However, the U.S. has not contended with a true technological peer competitor for thirty years. Over the last decade, alarm bells have rung more and more loudly and insistently about the threat to U.S. power projection posed by Chinese and Russian military modernization. My voice helped to start that process in 2010 when I returned to government after a 15-year absence. Despite this growing recognition, I believe the U.S. is not gaining ground yet in the competition for conventional military superiority. We may not be prepared to embrace the degree of change that warfare's independent logic is going to impose on us. Change brings risk, but so does complacency and inertia.

Certainly, steps have been taken, going back to the Obama administration, to address Chinese and Russian A2AD initiatives. I don't believe those steps are adequate, largely because too many of them have been in the wrong direction or focused on the wrong problems. The U.S. has taken three strategic approaches to respond to the emerging conventional force threat to our power projection capabilities. First, the U.S. has sought alternative sources of technology, largely be reaching out to the commercial start-up world symbolized by Silicon Valley. Second, the U.S. has tried to accelerate the fielding of new systems through higher risk "rapid" acquisition approaches. Third, the U.S. has embraced a largely aspirational goal of integrating operations through advanced information and artificial intelligence technologies. All three of these initiatives have positive attributes and can provide improvements in fielded capability, but at least as implemented, none provide the kind of next generation game changing capability the U.S. actually needs. In some cases, they are making the problem worse. The outreach to commercial technology sources for innovation may accelerate the flow of some technology into the Defense Department inventory, but competition among defense contractors already provides strong incentives for this to happen and the innovation that's missing is on the requirements side of the house—the demand side—not the supply side of the so-called "valley of death." Overly aggressive development schedules are more likely to lead to program failure, higher cost, longer schedules, and lower quality products than they are to revolutionary capability fielded dramatically faster (there are decades of experience and data to support this). Integrated Joint C2 do not appear to be well-focused and will

[81] After Crecy and Agincourt mounted armored knights spent decades trying to improve armor and outlawed crossbows rather than accept the end of their status as elite warriors.

not make current systems and assets significantly more survivable. There is only one way to change the trajectory the U.S. is currently on; that is to determine what the next generation of conventional warfare will look like and to get there first. I don't believe it will look like improved versions of the things we already have, even if they are integrated more effectively. Running faster in the wrong direction will not get us where we need to go; it just consumes our most precious resource—time.

I am convinced that unmanned lethal autonomous systems, operating in conjunction with one another, and which have roughly the characteristics I have described in this paper, will be that future generation. Over the months I've spent writing this paper, the evidence this is where the future of warfare lies has only increased. I am equally certain I haven't got the specifics of those concepts right, but I have provided a reasonable starting place for thinking about, analyzing, modeling, and experimenting with these ideas and others. The U.S. needs to get on with that work on an urgent basis. It also needs to happen in secret as much as possible. We have been far to open about our ideas and our plans and about the specifics of the systems we place in development. Relative time to market is everything when one is engaged in a highly competitive enterprise, and in the words of one of my favorite fiction writers, "We don't have a moment to lose."

If I'm somewhere near correct in the view that lethal autonomous systems will to a large extent replace humans and human crewed systems in future conflicts, then there are some questions we should try to answer and some implications we should consider:

> Both conflict initiation and conflict termination may be fundamentally different—or not.
>
> Escalation might be very hard to control.
>
> The first mover advantage could be highly destabilizing.
>
> Superiority in AI-aided or autonomous operational decision making could (would?) be decisive.
>
> Either space or cyberspace could be the decisive domain.
>
> Conflict length could range from very short to very long depending on relative advantage and on incentives to de-escalate.

Various risks could provide powerful deterrents to future conflicts. These include escalation to nuclear war, economic disruption, loss of societal control by established elites, the potential for unforeseen catastrophic operational failure or conversely for a lengthy and industrialized war of attrition. But, cutting the other way may be the potential perception, real or imagined, that geopolitical or other desired end states can be easily achieved by initiating a short decisive conflict from a position of technological superiority, possibly by surprise.

Let's all hope these questions and implications are moot, and the future of warfare is a null set. War is a stupid and wasteful mechanism for solving disputes among humans. Unfortunately, the alternatives require some willingness to accept a partial loss of control over decisions—acquiescence to the rule of law in some form. Over the centuries of human civilization, the rule of

law has gradually expanded to replace personal vendettas, feuding between clans, violent conflicts between city states, and most but not all tribal warfare and religious warfare. Attempts to establish mechanisms to eliminate wars between nations have made some progress, but the specter of large scale conventional, and even nuclear conflict still haunts us all.

Autonomous machine-based or not, the future of warfare will still depend on human decision making about starting wars. Unfortunately, the raw material of human psychology and its manifestations in society's collective behaviors and in individual human leaders hasn't changed much over the handful of centuries of human organization in large societies. With the movement toward conflict occurring primarily between autonomous machines instead of between human beings in crewed platforms I anticipate in this paper, perhaps the folly and irrationality of not having other non-violent mechanisms to resolve our differences will become clearer and more compelling. I fear the result will be the opposite.