AIR WAR COLLEGE

AIR UNIVERSITY

AN ANTIFRAGILE APPROACH TO PREPARING FOR CYBER CONFLICT

by

Lance Baxter, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Panayotis Yannakogeorgos

5 April 2017

DISCLAIMER

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

Biography

Lt Col Lance Baxter is assigned to the Air War College, Air University, Maxwell AFB, AL. He previously served as the Lead IMA for the Missile and Space Intelligence Center, Defense Intelligence Agency, Redstone Arsenal, Alabama. As a civilian, he works in the Lead Development Test Organization for the Ground Based Strategic Deterrent System Program, at Arnold Air Force Base, Tennessee. He also served as IMA to the Deputy Program Manager, C-130 Avionics Modernization Program Warner Robins AFB, manager of the space environments test team at Arnold AFB, and Space Electronics Engineer in the passive sensors branch of the space sensors division, Air Force Research Laboratory, Kirtland AFB. Lt Col Baxter deployed to Baghdad, Iraq in 2010 in support of Operation Iraqi Freedom and Operation New Dawn. As a civilian, he served as Squadron Director for the 649th Test and Evaluation Systems Squadron, and Branch Chief for the Test Technology Branch.

Abstract

"Defense" of any system against all highly improbable, but significant events, what are sometimes referred to as Black Swan events, is not possible. These events are, by their very nature unpredictable and uncertain, which is why they so dominate our thinking, and our culture. The work of Nassim Taleb regarding these highly improbable events and his proposed approach of "antifragility" may have utility in studying what the USAF should do in order to be prepared for the future in cyber operations. This approach emphasizes the futility of trying to predict when/where and how these highly improbable but significant events will occur and of preparing to defend against those scenarios. This leads to a "barbell strategy" based on an understanding of the probability and consequence of both positive and negative Black Swan events, which maximizes optionality while ensuring against systemic failure.

Three essential elements emerge from this as critical to building "antifragility" into our national cyber capabilities. The first is the need to truly understand our minimum required capabilities, to acknowledge what ruin would really look like so that it can be avoided at the lowest possible cost. Second, how can optimal learning be built into the system, allowing the inevitable shocks of any magnitude to make the system stronger. Finaly, what construct, organization or approach can efficiently and effectively incentivize the high-risk/high-payoff end of the spectrum.

There is a demonstrated history of throwing around Pearl Harbor and the attacks of 9/11 as cyber scenarios to defend against or prepare for. In this assessment, the potentially more helpful analogies of the Battle of Britain and the Maginot Line will be evaluated as well. This will help to examine the potential application of "antifragility" and the associated "barbell strategy" to USAF strategic preparations for conflict in the cyber domain.

Introduction

The United States is arguably the most internet dependent nation on Earth, and our military is keenly aware of the risks that this dependence poses. A quick internet search of "cyber Pearl Harbor" and "cyber 9/11" shows that these concepts have been publicly discussed since at least November 1997, when Deputy Secretary of Defense John Hamre testified to congress about the dangers of an "electronic Pearl Harbor".[1] In later interviews, he credited Air Force General Tom Marsh with "authoring the phrase"[2]. There is a vast array of published work on both "cyber Pearl Harbor" and "cyber 9/11" that indicates there is no shortage of awareness something dire might happen in cyberspace. Even Secretary Hamre has acknowledged that it may not have been the best analogy to use at the time he first introduced it.[3] Almost invariably, these terms are used to demonstrate that we should be doing something different in order to avoid or defend against the cyber-equivalent of those traumatic events. What do "cyber Pearl Harbor" or "cyber 9/11" even mean? Beyond the scare tactic of bringing up a traumatic event from our collective social memory, each of these scenarios can be seen to represent a different type of unanticipated attack on the United States. What is lost in the sensationalism that often surrounds bringing up these analogies is that they actually can represent scenarios that should be deeply and carefully considered, but not necessarily in the way that scare-mongers would suggest. The utility of scenarios in understanding different aspects of cyber conflict is not limited to these two oft-cited examples. There are other analogies in the recent history of warfare that we should also draw upon to help understand how to prepare properly for combat in this new domain.

Thesis

This research paper proposes an alternative approach to weighting the strategic investments to be made in Cyber capabilities across the DOTMLPF-P spectrum to reflect a "barbell strategy" suggested by the philosophical theory of Dr. Nassim Taleb described as "antifragility". This approach is evaluated in light of four scenarios, a "cyber Pearl Harbor", a "cyber 9/11", a "cyber Battle of Britain", and a "cyber Maginot Line", to determine its possible utility.

Cyber Strategy Viewed Through Historical Analogies

In this examination, the Pearl Harbor analogy will be used specifically to evaluate state-on-state protracted warfare that begins with a crippling first strike. Pearl Harbor was a surprise military attack on the US naval and air forces in Hawaii on 7 December 1941. Pearl Harbor represents an unanticipated military shock delivered to the US military forces by another sovereign nation. The bulk of the US Pacific Fleet was stationed at Pearl Harbor, as were most of the Army Air Corps aircraft in that theater. These two concentrations of assets represented the majority of the military hardware that could be used in the short term to strike against Japan. A surprise blow to these military capabilities was intended to so cripple the US militarily that the Japanese would be able to then be able to defeat the US in war. It was devastating to the US Pacific Fleet, and many Americans lost their lives. However, just over 6 months later, Lt Col James Doolittle led a bombing raid on the mainland of Japan, and by 16 August 1945 the Empire of Japan surrendered to the United States. The shock to the system that Pearl Harbor represented did not break the United States Navy, the Army Air Corps, or the United States as a nation. Rather, the events of WWII catapulted the United States onto the world stage as one of two superpowers that would dominate international affairs for a half century, followed by decades of unipolar dominance by the US following the fall of the Soviet Union. Thus, Pearl Harbor revealed the "antifragile" nature of the US military, our society and our government.

In this examination, "cyber 9/11" will be used to examine a surprise attack on civilian targets/infrastructure by a non-state actor, and the resulting response. The "cyber 9/11" analogy has been used since at least 2011, and has gained significant popular attention. Often used as a sort of shorthand for cyberterrorism, it touches on a particular concern of the United States as we

press on in a decades-long "war on terror". This analogy refers to the unanticipated and asymmetric attack on American civilian targets/infrastructure by a non-state actor for the purpose of sowing chaos and fear. It is important to note, that while thousands of innocent civilians lost their lives in the attacks on 11 September, 2001, the United States was not defeated, and in fact, the organization directly responsible for the attacks has been effectively dismantled, and all of its senior leadership from that time have been captured or killed. The attacks on 9/11 and the US response to them also demonstrated the "antifragile" nature of the US economy, culture, and government as they were not destroyed by the attacks. In fact it can be argued that all of them have gotten stronger because of that shock. Demonstrated in part by the fact that we have not suffered another catastrophic terrorist attack within the US since then.

As we compare strategic approaches through the lenses of these two analogies, it is important to note that they actually may not be particularly helpful. Neither example resulted in a defeat of the United States, in fact it could be argued that both of them actually represent positive examples of "antifragility". American military power in the case of Pearl Harbor was not shattered by the attack, but rather improved because of it. The use of multiple instruments of American national power resulted in the death or capture of all of the individuals behind the attacks on 11 September, 2001 and the US has not suffered another significant terrorist attack against our civilian population since then. Because of the deficiencies in these two commonly used analogies, we will consider two different, and possibly more pertinent analogies. The first of these is the Battle of Britain.

In this case, the technologically and numerically superior German Luftwaffe[4] were defeated in their attempt to gain air superiority over the English Channel in preparation for Hitler's planned invasion of the British homeland.[5] This is an example of state-on-state total war

for national survival in a relatively new operational domain. The rate of innovation, the determination, and the operational flexibility of the British and their allied forces which Wood and Dempster refer to as "controlled scientific warfare" [6] ultimately carried the day. As we search for useful analogies to assess US preparations for cyber conflict, ensuring that we are preparing to win a "cyber Battle of Britain" could be one good place to start. While it ultimately demonstrated the "antifragility" of the British people and the allied military forces, it was a more immediate and protracted threat to national survival than either of the first two examples.

Perhaps the most stressing, and therefore important, analogy that we could use to assess US preparedness for cyber conflict is that of the French commitment to the Maginot Line in the time between WWI and WWII. In the National Defense University Press Joint Forces Quarterly, Marine Major Clifford S. Magee presented this analogy to be considered in cyber conflict, the "cyber Maginot Line".[7] In his argument, he uses this analogy to call into question the reliance on firewall technology in the defense of computer systems. This is appropriate, but is a more limited treatment than we will undertake. In this examination this example will be extended to an overall strategic approach to preparation for cyber warfare. The Maginot line represents a cautionary example of the danger of investing the bulk of your resources in a single system or strategic approach. These are what Dr. Taleb would describe as "fragile", susceptible to breakage when exposed to an inevitable but unexpected shock. This inappropriate investment in a single system and strategy ultimately led to the defeat of France at the hands of the Wehrmacht in a matter of six weeks.[8] In proposing a strategic approach to assessing US preparedness for cyber conflict, ensuring that we are avoiding the analogous results of the French reliance on the Maginot Line is critically important.

Current US National Cyber Strategic Approach

The need to protect critical infrastructure, sensitive unclassified and classified data, and Command and Control systems that operate in the cyber domain is well documented. USCYBERCOM stood up on 23 Jun 2009, and the 24th Air Force was designated AFCYBER on 7 Dec 2010. The mission statement of 24th Air Force/AFCYBER, is "Operate, Extend and Defend the Air Force Information Network, defend key mission systems, and provide full spectrum capabilities for the Joint warfighter in, through, and from cyberspace."[9] Planning documents such as the Joint Operating Environment 2035 (JOE 2035) identify what future conflict environments and challenges might be. JOE 2035 in particular identifies "context five", described as the Contest for Cyberspace, a "*struggle to define and credibly protect sovereignty in cyberspace."*[10]

The USAF Information Dominance Flight Plan "provides the overarching guidance and processes for unifying Air Force cyberspace initiatives over the next 10-years, and it is built on the foundation of the Air Force's Strategic Master Plan and Future Operating Concept to ensure unity of action and effort toward fully exploiting cyberspace."[11] It defines "Information Dominance: The Air Force fully exploits the man-made domain of cyberspace to execute, enhance, and support Air Force core missions."[12] In this document, it is noted that "Command and Control (C2) is essentially about information: getting it, judging its value, processing it into useful form, acting on it, and sharing it with others. There are two basic uses for information. The first is to help create situational awareness (SA) as the basis for a decision. The second is to direct and coordinate actions in the execution of the decision. (Joint Pub 6-0)."[13] Trusted information and resilient and trustworthy systems form the core of the military requirements to support Information Dominance. Resilience is described in *50 Cyber Questions Every Airman*

Can Answer, Number 38: How do Systems Survive and Recover from Attacks? "At the system of systems level, hardware and software diversity increases the ability of a complex system to survive a discriminating attack against a specific class of systems. A zero-day exploit targeting an un-patched vulnerability inflicts more damage on a vulnerable homogeneous system than it does against a diverse heterogeneous system with a mix of machines. A layered defense in depth makes allowance for successful attacks, and sets in place procedures for post-threat recovery. Cyber attacks result rarely in permanent destruction of systems that necessitate hardware replacement. In either case, recovery necessitates pre-established systematic procedures to restore a system to a known stable state."[14] Resilience is necessary, but not sufficient for establishing "antifragility". Resilience ensures that a system survives the shocks that it will experience, but the learning characteristic that allows it to grow stronger from each shock is the critical additional factor that differentiates "antifragile" from merely resilient.

Associated with these concepts is that of Mission Assurance, which is defined in DoD Directive 3020.40 as "A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition."[15]. According to DoDD 3020.40 "DoD uses MA as a process to protect or ensure the continued function and resilience of capabilities and assets by refining, integrating, and synchronizing the aspects of the DoD security, protection, and risk-management programs that directly relate to mission execution."[16] This fundamentally links Information Dominance, Mission Assurance, and Risk-Management together in a way that feeds the requirements processes for organizations, acquisitions, personnel actions etc.

According to the DoD RIO "Risks are defined by (1) the probability (greater than 0, less than 1) of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur."[17] This has the effect of limiting consideration to those risks that are of moderate or higher probability, ensuring that Black Swan events are not significantly considered in the risk assessments that are performed, because their probability is so close to zero. The reliance of the Mission Assurance process on this risk management framework biases it away from considering both highly improbable bad events and those that might be beneficial. Rather, it is focused on the more likely, less significant "moderate" risks.

We have known issues in the information domain. The Government Accounting Office found that, "for fiscal year 2014, 19 of the 24 federal agencies covered by the Chief Financial Officers (CFO) Act reported that information security control deficiencies were either a material weakness or a significant deficiency."[18] Not a rosy picture when so many agencies know that they have "material weaknesses or significant deficiencies". What should perhaps be even more worrying is that this doesn't even begin to account for issues that the agencies don't know about. These issues are fundamentally what we are to consider in contemplating a "cyber Pearl Harbor", "cyber 9/11", "cyber Battle of Britain" or "cyber Maginot Line.?

One thing that stimulates an active public discussion of these threats and this new battlespace is that there are already engagements and casualties taking place, and many people are not quite sure what to make of them. Russian hackers "break in" to the publicly available voter registration databases in two states and download information that they could easily have requested and received semi-legitimately.[19] State-sponsored groups breached Sony Pictures Studios and did millions of dollars in damage.[20] All of this tends to further reinforce the focus of the current approach on "moderate" risk, foreseeable events in the near-to-mid-term which can

potentially be mitigated by specific investments along the DOTMLPF-P spectrum. This distracts attention and resources from the areas that the "barbell strategy" suggests are the most important, the very low risk approach to eliminating the risk of ruin, the highest-possible risk/reward investments, and enabling learning at all levels within the system.

"Antifragility" Applied to Planning for Cyber Conflict

Outliers are events that most of the well-understood and commonly used statistical tools and processes discount, or exclude from their datasets in order to mathematically analyze them. For the simple Gaussian statistical approach to work, there is an acknowledgement that there are events that are vanishingly unlikely. In practice, however, if one of them is observed, it generally must be removed from the data-set in order to enable analysis based on the assumption of a Gaussian Curve, "One single number can disrupt all your averages".[21] How then, can we account for these events that we know occur, but our tools cannot account for? There is a unique intersection of psychology and statistics that makes these particular kinds of events that are statistically unlikely, but which have overwhelmingly significant impact even more difficult. In his book *The Black Swan: The Impact of the Highly Improbable*, Dr. Nassim Taleb describes one aspect of this challenge, the "problem of induction" using a story of the life of a domesticated turkey. For one thousand days, the turkey gets fed and cared for consistently by the farmer in what seems to the turkey to be a very predictable routine. Being slaughtered, rather than fed and cared for on the one thousand and first day is a Black Swan event for the turkey. Applying inductive reasoning to all of the data available to the turkey at the beginning of day one thousand and one would indicate that the turkey should be accurate in predicting that day will be just like every other day that has been observed up to that point.[22] In fact, this exposes one aspect of the nature of these events, they are not predictable by simple observation and induction, and therefore arguing for or against their occurrence using those techniques is futile and possibly dangerous. Because of this problem, it would be irresponsible to base our preparations for future cyber conflict strictly upon our observations of the environment and conditions around us now,

doing so could lead us to make fragile assumptions that will lead to collapse when exposed to the inevitable Black Swan events.

Prior to the Japanese attack in December of 1941, there wasn't a report by the Department of Defense stating that the US Navy reported that ¾ of the Pacific Fleet, and from the Army that most of its combat aircraft in the theater are at risk for attack at bases in Hawaii. In retrospect, some people have pointed to indicators that they suggest should have signaled that an attack was coming. There have not, however, been any predictive tools built based on those observations that are universally useful. There haven't even been any developed for accurately predicting when the next aggressive island nation bent on world domination is going to attack a major US Naval installation. Most importantly they haven't led to a model that can predict when and how some other adversary will discover a way to attack us in a completely novel way and then decide to use that against us. This lack of an ability to create useful predictive analysis from an observed event is one of the ways to identify that it is a true Black Swan. This same logic can be applied to understanding the attacks of 11 September, 2001 and the German invasion of France through the Ardennes forest as Black Swans as well. While the German air attack on the United Kingdom in the Battle of Britain was not in itself a surprise at that moment, it was certainly a stressing event that was not predicted by planners and statesmen years prior to the outbreak of the war, and it represents a non- Black Swan event which still demonstrates the value of an "antifragile" approach to military strategy.

A military analogy relating directly to the "problem of induction" described by Dr. Taleb[23] is that of the French reliance on the Maginot line. There was a lot of historical precedent that indicated that the Germans might attack France again. There was also a great deal of evidence that when they did, it would be across the shared border in the vicinity of Alsace-Lorraine where the terrain and conditions were ideal for the movement of large armies.[24] These two nations have thrown invasions back and forth across that same border for centuries. The French strategic position was based on inductive reasoning based on these observations. They built a theoretically impenetrable line of interlocking artillery, defensive emplacements, and observation posts, manned it with highly trained personnel, and prepared thoroughly for the anticipated coming attack.[25] This single-minded focus on the clear and logical threat vector, we now know, led to the fall of France at the hands of Hitler's forces in a matter of six weeks when the attack came through the Ardennes forest and across the Rhine rather than across the exquisitely defended line.[26] Like the turkey in Dr. Taleb's example, limiting our observation of what has been, and what is observable today, and the logical analysis of that data led to a fatally fragile strategic position.

Gaining a full understanding of what events are already being predicted and prepared for is, however, an important first step. It is fundamental to avoiding the risk of ruin. It is not enough by itself, and committing to more than the necessary level of investment to ensure survival consumes resources that could be invested to greater effect in high-risk/high-payoff game-changing approaches. Dr. Taleb describes this in his book *Antifragile: Things That Gain from Disorder*. "Antifragility" and the philosophical basis behind it, provide a usable starting point from which to attempt to build strategies that encompass his principles. Uncertainty drives all of this discussion, the uncertainty of the Black Swan events that inspire us to be concerned

about these events and the uncertainty of developing new approaches that will complicate enemy actions, simplify friendly force responses, or even render concerns of cyber-attacks obsolete. Managing such uncertainty in our personal lives is difficult, we buy insurance, make investments, choose where to live, what hobbies to do, who to marry and what cars to drive all based on our (often inaccurate) assessments of uncertainty. Instead of working to eliminate uncertainty, which is fundamentally impossible, taming it by the application of a "barbell strategy" is the methodology suggested which is suggested by "antifragility".[27]

A "barbell strategy" is fundamentally a bimodal approach with separate fundamental goals.[28] The goal of the first mode is the elimination of the risk of ruin. This is what drives the acquisition of insurance in our personal lives, it is fundamental to military training where service members train to survive even when deprived of all of the equipment and supplies, and in high-performance aircraft through the incorporation of ejection seats and parachutes. The second mode is to maximize the potential for what investment brokers and economists term "upside gains". This is the opportunity to benefit from an investment, whether that is in time, money, effort, or focus. Laboratory research, oil and mineral exploration, high-risk investing are all examples of this approach. Combining the two modes within an appropriate learning context results in a "barbell strategy". Dr. Taleb states that "a barbell strategy with respect to randomness results in achieving antifragility thanks to the mitigation of fragility, the clipping of downside risks of harm—reduced pain from adverse events, while keeping the benefits of potential gains."[29] It is important to note that this is not an approach to try to eliminate uncertainty, rather it is an approach that seeks to domesticate it and take full advantage of the benefits that it can provide while protecting ourselves from the potential for harm.[30]

By applying a "barbell strategy" to the USAF preparations in the cyber domain, we can also identify the most appropriate changes to make. The goal is to domesticate the uncertainties inherent in cyber conflict, eliminating the risk of ruin, and at the same time positioning the Air Force to benefit from improbable, but significantly impactful, discoveries across the DOTMLP-F framework. Understanding clearly what the definition of ruin is and making sure that efforts to ensuring that those capabilities that must be maintained are hyper risk-averse is key to anchoring one end of the barbell. Contrary to the usual answers given when programs ask operators what minimum requirements are, these capabilities must be literally what is needed for survival. Not what is needed day-to-day, or what is preferred to allow operations to proceed normally. This minimum acceptable level of performance must be defined carefully because if it is allowed to creep upward, it drives requirements that consume the entire budget and still cannot be achieved. After "clipping the downside risks of harm"[31] with this approach, the vast majority of the remaining available resources should be applied to the other mode of the strategy.

In this case, that means supporting research into game-changing technologies, finding and training individuals well outside "normal", and building organizations that allow and even encourage radical risk-taking in the pursuit of lofty objectives. The challenge here is similar to that faced in high-risk investing. How to create an environment that encourages innovation and rewards productive risk-taking? Think-tanks are one existing possible approach, but the incentive structure is wrong, and eventually perpetuates the organization rather than true innovation. Current USAF organizational research and development is often stalled by bureaucratic or organizational issues and sub-optimization due to structure and resourcing. The Defense Research Projects Agency (DARPA) and the Small Business Innovation Research (SBIR) program also represent attempts to get at this challenge, but they have their own

limitations in capacity and incentive structure as well. What is needed is a new approach that invests in the best people, empowers them to try radical things, rewards them when they succeed, and also rewards them when they fail and transmit the lessons they learned to the rest of the system.

The fundamental underlying characteristic of an "antifragile" system is that when it is shocked, it gets stronger or improves. This is not possible if there is no mechanism for feedback and for memory. In the biological systems that constitute some of the best examples of "antifragility", early death of individuals in a population is the feedback, and the DNA of the survivors is the memory. Selective reproduction of the survivors represents the learning function. As we strive to implement a "barbell strategy" in order to build an "antifragile" approach to cyber conflict, it is critical that at every level the capacity for learning is emphasized. This applies equally to software, where updates fix errors and threat signatures are added to databases, to development and training processes where best practices and successes are propagated across programs and taught to successive generations of practitioners, to operations where one team encountering a new threat or environment is in constant contact with all other operators so they know immediately about it and can start to learn what it means to their next operation. If the strategic approach to cyber conflict that is implemented fails to incorporate learning in all possible areas, it will not be able to gain from the various shocks that it will experience, nor will it be able to incorporate the game-changing developments which will result from the high-risk/high-payoff mode of the "barbell strategy".

Assessing the "antifragile" Approach by Analogy

Having looked to four analogies for inspiration in the beginning of this analysis, it is now time to return to them to understand how this approach might fare in each scenario. Cyber 9/11 – a surprise attack on National Critical Infrastructure by a non-state actor will certainly cause some damage, and potentially some casualties. The installation of resilient systems allows for critical functions to be performed, and reduces the initial impact of the attack, limiting the impacts geographically, systematically and/or temporally. Watching the events unfold, the whole nation understood, possibly even before Flight 93 was hijacked, that a new method of attack was possible. Airline passengers, pilots, flight attendants and Government officials all quickly adopted new perspectives, assumptions, and actions. So too will the learning organizations tasked with Cyber operations disseminate information, process it, and improve their functions based on what they can learn. In this way, though we will sustain some damage, and possibly some casualties, though hopefully no loss of life, Cyber 9/11 won't be the dreaded event that damaged our nation, but rather it will be just another historical event that has made us stronger.

Cyber Pearl Harbor, as mentioned above, is an unanticipated catastrophic nation-state attack on military infrastructure. If this were to occur in an explicitly "antifragile" environment, this is how such an attack might play out. *On December 7th, 2023 the military forces of the United States of America were suddenly and deliberately attacked by the cyber and air forces of North Korea. Having infiltrated our Combined Air Operations Center networks undetected, North Korean forces synchronized a DDOS attack on primary command and control systems with air attacks on US and ROK airbases in South Korea and Japan. Redundant command and control systems that are independent from the compromised capabilities were used to transmit*

critical warning orders and tactical guidance to forces at those bases despite the effective cyber-attack. Reduced bandwidth and the loss of key force-enhancing features of the primary systems resulted in significant, but not catastrophic casualties. After "sinkholing" the DDOS attacks, and taking control of the offending botnet, Defensive Cyber Operators were be able to patch, recover and operate the primary systems in very short order. At the same time, the attack vector used was blocked in every single US military and civilian critical infrastructure system. It was also made instantly available to Offensive Cyber Operators to exploit North Korean infrastructure systems in sectors unaware of the cyber-attack vector their own forces had used, partially enabled by their own botnet. Within a few days, now protected from this type of cyber-attack, waves of SEAD aircraft clear the skies, coordinating over the reconstituted primary command and control systems with strike aircraft that effectively eliminate all enemy air-to-air systems, surface-to-air capabilities, and elements of their national military industry, beginning the campaign to ensure the unconditional surrender of the attacking nation.

The cyber Battle of Britain scenario also demonstrates the value of key aspects of "antifragility". *As a peer competitor, in 2039 Russia has determined that it must establish firm dominance in the information domain prior to a conventional military invasion of the United Kingdom. In order to do this, all of the significant capabilities of the Russian national hacking capability are dedicated to taking the UK offline completely and utterly. British cyber-forces, equipped with a variety of different cyber weapon systems, operating on a number of separate and independent networks, work tirelessly to defend their nation. Legions of cyber operators executing well-understood DDOS attacks, phishing attacks, and crude infrastructure attacks. Within a few days, the British operators discover that the Russian forces are coordinating their attacks using chat rooms and IRC messaging services. Without revealing that they know how the*

coordination is taking place, British operators begin to monitor these communiques, and are standing by to shut down potentially sensitive systems, defend what must be defended, and hack-back with devastating effect. Passing information to each other instantly, the small but determined force of UK defenders is able to inflict such losses, and to keep enough UK cyber capability on-line that the aggressors eventually decide that an invasion must be postponed due to the inability to gain critical cyber-dominance in preparation for the assault.

Finally, the cyber-Maginot Line provides us with perhaps the best lesson of all. *In 2037, a byzantine failure analysis of the massively expensive "impenetrable barrier firewall" under development by USAF Cyber Lifecycle Management Center, revealed a critical vulnerability that would have allowed attackers to enter the nations critical infrastructure and Nuclear command and control systems unopposed. Implementing an "antifragile" approach, a number of distinctly different and redundant systems were developed and deployed to work in concert with each other and the primary system. Systems and operators were linked together in a way that knowledge about any enemy action is instantly available, as are innovations made by friendly forces, offensive or defensive. When the inevitable peer-competitor attack came through the avenue left vulnerable by the monolithic system, it encountered resistance immediately, which rapidly escalated into not just a repulsion of their attack, but rapid penetration and compromise of the offensive systems in use. As follow-on forces attempted to use similar tactics, techniques and procedures, and/or related cyber weapons-systems, the automatic patching and instantly updated heuristics recognized and neutralized their attack vectors before they could even begin their operations. The few operations that did manage to initially penetrate the wall encountered a maze of interlocked systems. Rather than finding wide open, undefended spaces beyond the initial firewall, they encountered active and adaptive defense, skilled and coordinated cyber*

hunters, and a disappointingly ever-more-difficult task just to maintain their initial positions in the contested space. Instead of a wave crashing around the edges of the wall and flooding the unprotected network beyond, their attack was absorbed, diverted, or turned back on the attackers' own systems, flooding them with the same digital attacks that they attempted to use.

Adopting a posture of "antifragility" in all of the aspects of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities is central to achieving the positive outcomes in each of the scenarios presented. It is not an answer to preventing attacks, or even to eliminating all repercussions from them. It is, however, a way to ensure that no cyber-attack destroys the U.S., and that every shock to our cyber systems makes us stronger, more capable, more secure, and more prepared.

Recommendations

A top-down review of all planned Air Force Space Command DOTMLPF-P investments to support US preparedness for cyber conflict should be executed to determine the current level of fragility looking for indicators such as non-learning systems and monolithic systems, training and thinking that represent potential systemic vulnerabilities. Next, an updated portfolio needs to be developed which deliberately increases optionality while as much as reasonably possible eliminating the risk of ruin in coming cyber conflicts. This effort requires the difficult task of defining what the minimum acceptable capability is for all DoD critical infrastructure, all sensitive data, and all C4I systems that rely on the cyber domain. It also requires a review of the entire portfolio of potential investments that can be made which represent the high risk end of the proposed bimodal strategy. This will require the establishment on more efficient, more effective organizations, processes and techniques for investigating high-risk/high-reward approaches, particularly those that are non-material in nature. Finally, a systemic focus on feedback, memory and continuous improvement must be established. This must be at all levels, from installed legacy software systems to MAJCOM staffs, and from individual operators to complex systems of systems.

Air Force Space Command should begin a full review of their planned investments across the entire DOTMLPF spectrum to deliberately implement a "barbell strategy" at the national level in preparation for the potential coming cyber conflict. In the area of Doctrine, Air Force Doctrine Document 3-12 (AFDD 3-12) states "The Air Force ensures it can establish and maintain cyberspace superiority and fight through cyberspace attacks at any time regardless if the US requires the use of military forces."[32] This is fundamentally vulnerable to many of the logical fallacies that give rise to Black Swan events. Understanding what the absolute minimum

required level of cyberspace capability is needed at specific points to enable specific operations is critical. Planning to ensure a well-documented "survival" level to allow specific operations is critical to properly allocating scarce resources. Open-ended doctrinal commitment to superiority anywhere, anytime leads to unbounded requirements that are not useful for planning, organizing, training, or equipping forces. A more appropriate guiding statement might be "The Air Force ensures that it can establish and maintain cyberspace superiority and fight through cyberspace attacks at the time and in the environment necessary to ensure mission capability, both when the US requires the use of military forces and the defense of critical systems and infrastructure."

Air Force Organizations supporting the presentation of cyber capabilities, whether organize train and equip units or combat forces, need to posess the level and speed of learning that is necessary for the system to grow stronger after each shock. Current structures that rely on publishing and requiring the reading of lessons-learned, or mission de-briefs are not sufficient. The speed of innovation in cyber operations requires that all USAF cyber-operators be integrated directly in communication with each other to ensure instantaneous dissemination of critical information across all operators, offensive and defensive. Current National Mission Team and Cyber Mission Team constructs, and the division between offensive cyber operations and defensive cyber operations creates stovepipes that increases vulnerabilities and reduces effectiveness. Training for cyber operations needs to include an introduction to the philosophy of "antifragile" operations. Personnel operating day-to-day need to understand and support this approach, as it will form the basis for many of their operational requirements for learning, for resilience, and for mission risk analysis.

The acquisition of cyber weapons-systems is perhaps the area where the greatest changes can take place. Misuse the Risk Management Framework for cyber acquisitions drives programs

to low-to-moderate risk, and fails to properly account for improbable but significant events. A more appropriate approach to determining what systems should be procured and deployed, and how they should be integrated needs to be based not on programmatic risk, but on the assessed risks to mission failure. Resources that are saved from these more appropriately scoped procurements need to be reinvested in the highest risk, highest potential reward research and development in order to ensure that the positive Black Swans are captured and domesticated by the USAF. This fundamental shift in material acquisition strategy from one of mission-based aspirational procurement that revolves around programmatic risk to one focused on ensuring minimum operational capability is attained, learning is enabled, and the USAF is positioned to gain from game-changing developments is perhaps the biggest change that adopting an "antifragile" strategic approach would require.

Personnel, Facilities and Policy are all elements of the supporting infrastructure that will need to be optimized to support the shift in focus for operations. Certainly, hiring the people we need is critically important. Recognizing that some of them will be people who are well outside the mainstream of thought, particularly military thought, is critical to enabling the high-risk approaches needed to ensure success. Facility and policy changes to accommodate the exact approaches adopted by the operators in the future will be required, but are difficult to prescribe in advance.

Conclusion

Incorporating "antifragile" strategic approaches into preparations for cyber conflict will enable U.S. forces to take full advantage of the inevitable Black Swan events that it will experience. Preparing to survive and learn from all conceivable shocks will ensure that no matter what success adversaries have, it will be short lived and ultimately will fail. Dedicating significant resources to the research and development of very high risk, potentially high payoff will result in future capabilities we can't even imagine today. Organizing units and training our warfighters to communicate and learn from everything that is going on in their domain, and supporting them with leadership, facilities and policy designed to emphasize this approach will enable their success. This is the most logical, and potentially the most successful approach to the appropriate protection of critical infrastructure, minimizing the loss of sensitive information, and guarantying continuity of capability to maintain command and control of forces now and in the uncertain future.

[1] John Hamre, "The 'electronic Pearl Harbor'," The Agenda, December 09, 2015, accessed April 04, 2017, http://www.politico.com/agenda/story/2015/12/pearl-harbor-cyber-security-war-000335.
[2] Ibid
[3] Ibid
[4] Derek Wood and Derek D. Dempster, *The narrow margin: the Battle of Britain and the rise of air power, 1930-40* (Westport, Connecticut, Greenwood Press, 1975 reprint of New York, McGraw Hill, 1961), 54.
[5] Ibid, 13.
[6] Ibid
[7] Major Clifford S. Magee, "Awaiting Cyber 9/11", *Joint Forces Quarterly*, Issue 70, 3rd Quarter 2013.
[8] Rudolph Chelminski, "The Maginot Line," *Smithsonian*, June 1997, 98.
[9] 24th Air Force Office of History, *24th Air Force Heritage Pamphlet: HISTORY OF HQ TWENTY_FOURTH AIR FORCE AND 624TH OPERATIONS CENTER*, 17 January 2014.
[10] *Joint Operating Environment (JOE) 2035*, 34
[11] USAF Information Dominance Flight Plan, February 2017, 2.
[12] USAF Information Dominance Flight Plan, February 2017, 1-3.
[13] USAF Information Dominance Flight Plan, 3.
[14] Dr. Kamal T. Jabbour, "50 Cyber Questions Every Airman Can Answer", Air Force Research Laboratory, 7 May 2008, 19.
[15] Office of the Under Secretary of Defense for Policy, *DoD Directive 3020.40, Mission Assurance (MA)*, 29 November 2016, 18.
[16] Office of the Under Secretary of Defense for Policy, *DoD Directive 3020.40*, 3.
[17] Office of the Deputy Assistant Secretary of Defense for Systems Engineering, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, June 2015, 3.
[18] Gregory C. Wilshusen, *Information security: cyber threats and data breaches illustrate need for stronger controls across federal agencies*, 9, accessed April 5, 2017, http://www.gao.gov/assets/680/671253.pdf.
[19] Andy Greenberg, "Hack Brief: As FBI Warns Election Sites Got Hacked, All Eyes Are on Russia," Wired, August 29, 2016, accessed April 5, 2017, https://www.wired.com/2016/08/hack-brief-fbi-warns-election-sites-got-hacked-eyes-russia/.
[20] Lisa Richwine, "Cyber attack could cost Sony studio as much as $100 million," Reuters United States Edition, December 9, 2014, , accessed April 5, 2017, http://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209.
[21] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2010), 245.
[22] Taleb, *The Black Swan*, 40.
[23] Taleb, *The Black Swan*, 41.
[24] Chelminski, "The Maginot Line," 92-93.
[25] Chelminski, "The Maginot Line," 93-95.
[26] Chelminski, "The Maginot Line," 92.

[27] Nassim Nicholas Taleb, *Antifragile: things that gain from disorder* (New York: Random House Trade Paperbacks, 2014), 165-167.
[28] Taleb, *Antifragile*, 159.
[29] Taleb, *Antifragile*, 166.
[30] Taleb, *Antifragile*, 167.
[31] Taleb, *Antifragile*, 166.
[32] Curtis E. LeMay Center for Doctrine Development and Education, *Annex 3-12, Cyberspace Operations*, 11, https://doctrine.af.mil/DTM/dtmcyberspaceops.htm

Bibliography

Chelminski, Rudolph. "The Maginot Line." *Smithsonian*, June 1997, 90-100. Accessed April 4, 2017. https://web.archive.org/web/20071202110359/http://www.dushkin.com/text-data/articles/23427/23427.pdf.

Curtis E. LeMay Center for Doctrine Development and Education, *Annex 3-12, Cyberspace Operations*, https://doctrine.af.mil/DTM/dtmcyberspaceops.htm

Greenberg, Andy. "Hack Brief: As FBI Warns Election Sites Got Hacked, All Eyes Are on Russia." Wired. August 29, 2016. Accessed April 5, 2017. https://www.wired.com/2016/08/hack-brief-fbi-warns-election-sites-got-hacked-eyes-russia/.

Hamre, John. "The 'electronic Pearl Harbor'." The Agenda. December 9, 2015. Accessed April 4, 2017. http://www.politico.com/agenda/story/2015/12/pearl-harbor-cyber-security-war-000335.

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

Office of the Deputy Assistant Secretary of Defense for Systems Engineering, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, June 2015.

Office of the Under Secretary of Defense for Policy, *DoD Directive 3020.40, Mission Assurance (MA)*, November 29, 2016.

McGee, Major Clifford S. "Awaiting Cyber 9/11." *Joint Forces Quarterly*, no. 70 (2013).

Richwine, Lisa. "Cyber attack could cost Sony studio as much as $100 million." Reuters United States Edition. December 9, 2014. Accessed April 5, 2017. http://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209.

Taleb, Nassim Nicholas. *Antifragile: things that gain from disorder*. New York: Random House Trade Paperbacks, 2014.

Taleb, Nassim. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2010.

USAF Information Dominance Flight Plan, February 2017

Wilshusen, Gregory C. *Information security: cyber threats and data breaches illustrate need for stronger controls across federal agencies*. Accessed April 5, 2017. http://www.gao.gov/assets/680/671253.pdf.

Wood, Derek, and Derek D. Dempster. *The narrow margin: the Battle of Britain and the rise of air power, 1930-40* (Westport, Connecticut, Greenwood Press, 1975 reprint of New York, McGraw Hill, 1961)