Mission Assurance through Integrated Cyber Defense

Col William D. Bryant, USAF

Adversaries increasingly contest the ability of the United States Air Force to accomplish its missions in and through the cyberspace domain. Although different communities within the service focus on various approaches for a cyber defense framework, the best way to assure the Air Force's core missions is through a combination of defense in depth, resiliency, and active defense. Each approach is necessary, none is sufficient, and the service should combine them into a coherent whole for maximum effectiveness.

The core missions of the Air Force are heavily dependent upon freedom of action within the cyberspace domain. Unfortunately, we designed most of the weapons and missions systems in use today for a pre-Internet world. The implicit assumption was that our systems would operate in a fundamentally permissive cyberspace environment and that the greatest threat would be enemy signals intelligence.[1] The

Air Force designed many of its systems decades ago, so it is certainly not surprising that no one could predict the explosive growth and importance of the cyberspace domain. When system architects considered some form of information security for weapons systems, engineers normally assumed that border network defenses would keep out adversaries so that the environment seen by the weapons system would remain permissive and protected within network defenses.

These implicit assumptions have proven dramatically false. The pace of cyber attacks increases daily across the military, government, and civilian sectors. Cyber physical systems, those that include both physical and cyber components, are no longer safe—witness the successful attacks on industrial control systems and vehicles.[2] These trends are well understood and obvious. Making the situation dangerous is the fact that our adversaries also clearly understand our vulnerability to these types of attacks and emphasize them in their official published doctrine.[3] Just as our adversaries have come to think differently about warfare in cyberspace, so must we adjust our perspective.

The presence of a maneuvering enemy within the cyberspace domain requires a fundamentally different approach that goes beyond static defenses based on information technology (IT). Viewing cyberspace as a domain of warfare helps us understand why this is so. Carl von Clausewitz, the famous theorist of war, viewed warfare as two wrestlers, each trying to throw the other while constantly adjusting and reacting to the subtlest of movements by his adversary.[4] Static approaches that do not address what the enemy is doing will fail because he will react to whatever we have done to nullify their effect.[5] Mission assurance in and through cyberspace is not fundamentally an IT problem but a mission problem that requires a mission focus and approaches that go beyond what we have come to think of as traditional cybersecurity. Part of this perspective is to grasp that cyberspace reaches much further than traditional IT and into cyber physical systems upon which we rely.

Cyber Physical Systems

All modern systems exist simultaneously in both the physical and cyberspace domains. Opening panels on a modern fighter aircraft, for example, will reveal a large number of electronic boxes connected by wires. Those boxes generally do not use the standard transmission control protocol (TCP) / Internet protocol (IP) network protocol; rather, they pass information across data busses to other electronic boxes, clearly fitting the definition of cyberspace noted in Joint Publication 3-12 (R), *Cyberspace Operations*.[6] As noted in more detail later, any defender who takes comfort in the fact that those electronic boxes are not directly connected to the Internet but are "air gapped" should think again. He or she must realize that in almost all cases, those systems are actually connected to everything via several degrees of separation that attackers have demonstrated the ability to jump across via numerous methods.[7]

Since weapons systems such as ships and aircraft rely so heavily on cyberspace, actions within the cyberspace domain directly affect war-fighting systems in the physical domains. Adversaries can attack these systems in cyberspace through

numerous access points. Essentially, any physical connection that passes data or any antenna with a processor behind it is a potential pathway for an attacker. Obvious examples include maintenance and logistics systems, software-defined radios and data links, and other cyber physical systems that operators can connect to platforms, such as pods or weapons. To make things even more complex, these vulnerabilities are not static but change constantly.

Every software update, every new capability, and every novel piece of equipment can introduce new vulnerabilities. Defenders cannot simply "fix" a system and walk away, expecting the system or capability to stay "fixed." Furthermore, the weapons system platform itself may be completely secure, but maintenance, support, and logistics systems may prove just as critical to mission accomplishment. Squadrons of the most modern fighter aircraft with no fuel are nothing more than very expensive targets. Increasing complexity further is the fact that many critical mission dependencies lie outside Air Force boundaries in commercial systems such as power and transportation over which the service has very limited or no control. In some operational contexts, allied nations operate those systems with their own rules and priorities, making it even more difficult to influence how those countries protect the systems on which the Air Force relies. Since the range of vulnerabilities is so overwhelming, we must start by determining what is most important.

Key Cyber Terrain

To determine our key cyber terrain, we have to consider both the types of cyberspace assets we are examining as well as the level of analysis.[8] The three types of assets are traditional IT, operational technology, and platforms. Traditional IT systems include networks such as Nonsecure Internet Protocol Router (NIPR) and Secure Internet Protocol Router (SIPR) as well as IT-based weapons systems, including the air operations center and numerous other personnel and logistics systems. Operational technology refers to computer-controlled physical processes such as industrial control systems or other types of control systems such as building automation or heating, ventilating, and air-conditioning.[9] The latter category is a relatively new one in military circles but has attained wide acceptance in the civilian world. The final category, platforms, includes both an F-16 fighter and an Aegis cruiser. Cybersecurity experts tend to be very comfortable and familiar with traditional IT, are just starting to concentrate on operational technology, but have not yet really begun to figure out how to secure platforms.

Simply categorizing the type of asset is not enough. When determining key cyberspace terrain, an analyst should also look at three different levels of analysis and consider the component, the system, and mission levels. If our priority is mission assurance, then we will also have to move our analysis above the component level, through the system level, and finally up to the mission level. Even a relatively simple mission such as defensive counterair is enormously complex at the mission level when one analyzes the nodes and interdependencies. A fighter aircraft must be on station but must also have weapons. Where did those weapons come from? What systems were necessary to transport and load them? Are those

transportation systems protected from cyber attack? Each question leads to more questions; mission owners and analysts will have to work together to determine the most critical assets that will ensure mission success. Once analysts have completed their mission analysis, senior leaders will have to determine which missions are most important so they can decide how to allocate resources among them. What is more important—air and space superiority or rapid global mobility? Is global strike more important than intelligence, surveillance, and reconnaissance? Since the number of vulnerabilities is so vast, we will have to use our limited resources carefully for maximum effect.

Different Perspectives

Even after we direct our efforts toward the most significant vulnerabilities, a substantial problem remains. Various communities see cyberspace through very different lenses, based on their organizational culture and experience. It is a bit like the old fable about multiple blind men examining an elephant and coming to assorted conclusions about what it is like. Each blind man is correct about his particular area of the animal, but none of them understands the complete picture. Terminology confusion certainly does not help because "cyber" means different things to different people.

All of these factors lead diverse communities to put forward dissimilar approaches as "the" answer to mission assurance in and through cyberspace. Traditional IT communities favor utilizing defense in depth and providing multiple layers of static IT-based defenses. These communities tend to rely on compliance and security; some go so far as to equate compliance with security, believing that if evaluators check everything off the right checklist, then the system in question is secure. Acquisition communities tend to take a very different view, preferring to build resilience into systems instead of trying to retrofit security later. They create adaptable, resilient systems, and their greatest difficulty often lies in finding the right contract language that forces vendors to truly build in resilience—something notoriously hard to define. Cyberspace operations communities take a third and quite different view of how to provide mission assurance, turning to active defense through continuous monitoring and response to attacks. This emphasis on cyberspace maneuver, which relies on high-end operators and tools, can be extremely arduous to implement outside traditional TCP/IP-based networks.

All three approaches have great value; they are not exclusive but complementary, and any robust defense must include all three—integrated to support each other. Such integration offers a sustained competitive advantage that our adversaries will find difficult to replicate because of differences in culture. The Air Force has decades of experience in operating jointly and in teams with members from many services and backgrounds while most of our potential opponents are still used to operating within traditional service stovepipes. Each type of defense asks fundamentally disparate questions; requires completely different approaches, tools, and skill sets; and provides critical capabilities not found in the other approaches.

Defense in Depth

Without solid, basic IT-based defense in depth, too many attackers will get through, bring down even resilient systems, and overwhelm defenders. Regular firewalls and IT-based defenses may not stop high-level attackers, but they do eliminate the bulk of lower-level strikes and allow defenders to concentrate on the few high-level attackers who get through. This attrition of the majority of strikes is also critical for resiliency since it reduces the amount of damage sustained that the resiliency approach must overcome to allow the mission to continue. The fundamental question asked of defense in depth is, how can this approach make it hard to attack my systems successfully?

It does so by adding layers of defense, much like a castle with multiple walls. To borrow a term from cryptology, the work factor (i.e., the effort expended to penetrate defenses) is perhaps the most appropriate way to measure defense in depth.[10] Lining up 10 of the same firewalls with the same vulnerability is not nearly as useful as utilizing 2 different firewalls that require diverse techniques and tools to exploit. Most defenses in this area are technology based, including firewalls, intrusion-detection and prevention systems, blacklisting, whitelisting, and many other technologies and approaches.

A good defense in depth consists of several components. Border defenses make up its outer shell, keeping out low-level or "script kiddie" attacks, so named because unskilled hackers using prepackaged tools or scripts usually execute them. It is not sufficient just to have one or even several layers outside a network or system. Once an attacker gets in, the defender should still block him with multiple internal barriers. Defenders should configure these barriers to prevent lateral movement, privilege escalation, and the exfiltration of sensitive data. Vulnerability management across enterprises is also part of good defense in depth. To eliminate large sections of attack surface, administrators and architects should not only close vulnerabilities but also shut down unnecessary processes and applications. Of course, talking about reducing attack surface is easy, but doing it is very demanding because it often involves removing functionality and ease of use. Normally, all of these components are most effective if system architects build them in from the beginning or have them "baked in" instead of "bolted on" afterwards. To do so calls for good, secure systems engineering that considers security throughout the design process and looks both inside the system and outside at the environment in which that system is likely to operate. Starting in the design phase is actually too late; instead, systems engineering should begin in the requirements phase. Unfortunately, no matter how many layers defenders add, defense in depth has not always been successful against determined attackers.

Although necessary for any successful defense, static defenses are not sufficient; dynamic, determined attackers always seem to find a way into targeted systems. Modern systems are exceptional at making connections and thus creating attack surface. The potential area of vulnerability of even relatively simple IT systems is vast. For critical systems, an extreme version of defense in depth is an air-gapped system, in which architects not only have protected various possible attack vectors into it but also have tried to eliminate them by physically isolating the system with

no direct connections to less trusted systems. It seems that this approach would be foolproof, but in practice it is extremely challenging to implement.

In most cases, such systems are not truly air gapped because maintaining them requires connecting other maintenance systems to update or change them. Only rarely would developers update and write software that always stays within the single proprietary system. System administrators might think that their systems are truly air gapped, but an analysis of them by trained computer forensics personnel would normally demonstrate otherwise. Even if administrators were careful enough to actually air-gap a system with no leaks, in most cases that action would dramatically limit functionality. After all, the entire point of most systems is to share and process data. A computer may be "safe" if it is unplugged, buried 100 feet underground, and wrapped in 6 layers of duct tape—but it is also useless.

Finally, it is worth mentioning that a cyber physical system needs its own defenses under defense in depth. Such a system should have some defenses that do not rely on a particular host network; in aircraft, for example, the system is highly mobile, and operators and maintainers may plug it into different networks. Even if that is not the case, assuming that 100 percent security will be provided by any particular defense is not prudent. Security architects not only must plan ways to keep adversaries out but also should design the system to function even with the enemy inside.

Resiliency

Given that no defense will be perfect, systems must be able to function and carry out their missions with an enemy disrupting and attacking with some level of success. At this point, mission resiliency steps forward and makes it difficult for an enemy to realize his objectives. The Department of Homeland Security's Risk Steering Committee defines resiliency as the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[11] Resiliency allows for a less-than-perfect defense that still accomplishes the mission, even under attack in a cyber-contested environment.

Network and system engineers should plan for enemy success and expect it. They should avoid single points of failure and easy targets that enable an adversary to easily disrupt mission success for an organization. A mission system should be flexible and able to deform under pressure yet still perform its mission—much like a flexible bamboo stalk rather than a rigid oak tree.[12] It is of key importance that the mission, not the system, remain the objective of resiliency; resilience in cyberspace may lie completely outside cyberspace. Tactics, techniques, and procedures may fill in for technical defenses. For example, if an adversary disrupts a logistics system but logisticians on the ground use pencils and clipboards to figure out a way to get supplies to the right place, then a backup procedure has provided resiliency that had nothing to do with IT-based defenses. Another example: if an enemy attacks all of a squadron's smart weapons and renders them inoperable through cyberspace but the squadron switches to unguided munitions and destroys the target anyway, then the squadron has assured the mission despite the failure of some systems.

Mission resilience is designed to accomplish the mission under attack—much like a battleship continues to fight after taking numerous hits. Of course, there are many ways to implement technical and procedural resiliency. Designers build battleships with thick armor and watertight compartments to reduce the possibility of catastrophic damage when enemy shells strike. Designers can include comparable features in resilient IT and cyber physical systems.

Creating resilient systems involves a number of approaches that analysts can group broadly as multiple mission pathways, segmentation, and diversity. Multiple mission pathways make it difficult for an enemy to prevent mission accomplishment. For example, if an enemy disrupts critical system A, is there a system B that can replace its functions? Multiple mission pathways do not refer only to redundancy; system B can be a completely different type of system or no system at all if a procedure B replaces the function via some non-system-based method such as manual tracking. To create multiple mission pathways requires a significant change of mind-set away from efficiency. A completely efficient system has no redundancy or "wasteful" duplicative capabilities; a resilient system or process must have those things to prevent single points of failure. In a battleship, multiple mission pathways are the different ways that operators can maneuver the ship. The rudder is the primary mechanism, but if it fails or an enemy destroys it, the ship can be roughly maneuvered by using differential thrust on different propellers. Multiple mission pathways are a good start but offer only robust resiliency if designers segment them from each other.

With segmentation, failures should be contained and not affect an entire system. In a battleship, one obvious method of segmentation occurs through separate watertight compartments. Four discrete engines do not provide robust resiliency if a single hit can flood and disable all of them. In the cyberspace domain, architects create segmentation through separate physical infrastructure and hardware as well as IT-based defenses to prevent lateral movement between various friendly network segments. One danger in current IT trends is virtualization. A mission owner may have 10 separate servers but not realize that all of them are actually on the same physical hardware. Virtualization has considerable advantages for resiliency, but architects should apply it in a manner that avoids single points of failure. Separating systems via segmentation is an important step; the final one is ensuring that these systems do not share the same vulnerabilities.

Utilizing a single operating system, type of hardware, or application produces a single point of failure that can extend across an enterprise and present an attacker with a major opportunity. Military strategist Edward Luttwak notes that with a thinking enemy, "homogeneity can easily become a potential vulnerability."[13] For our hypothetical battleship, multiple mission pathways and segmentation are generally sufficient because an attacker has no realistic way to take down an entire category of redundant systems at the same time. An enemy must destroy each main turret separately; he cannot easily destroy them all with one shot. In the cyberspace domain, it is possible to take out any number of the same systems using the same vulnerability that an enemy rapidly propagates across systems. If an organization

relies completely on a single build of a single browser to run its logistics systems, then a vulnerability in that browser could shut down access to all of those logistics systems. It would be better if designers allowed for two or three different browsers that can be used to access and manipulate the data. Of course, having too many different types of applications and operating systems is more commonly the problem in organizations. Such overabundance introduces a much greater number of vulnerabilities into the overall system. Architects must strike the right balance with a small number of well-defended systems instead of either single points of failure or large numbers of unsecured systems.

These approaches to resiliency will be expensive, so acquisition programs will not implement them until senior leaders make resiliency a priority and build it into the acquisition process. One difficulty in building resilience has not been in engineering or design challenges but in finding the right contract language that drives vendors to build truly resilient systems. Program offices measure the success of their program by cost, schedule, and performance. As long as those are the only components of a program's report card, mission assurance will continue to end up "below the cut line" and unfunded. It is possible that programs could capture mission assurance and resiliency under the performance metric, but previous acquisition programs have not prioritized these factors under performance. To force this prioritization, senior leaders must be willing to make some hard decisions and refuse to allow programs to move forward through milestones unless they have incorporated mission assurance and resiliency. Doing so will prove extremely problematic to implement because of the pressures of the acquisition process, but there are indications that some senior leaders are starting to take this approach. Those individuals illustrate that in cyberspace resiliency and mission assurance, people matter.

The most critical component of cyberspace resiliency and mission assurance most often lies outside cyberspace—with the human war fighter. People are what makes this work. This fact applies across the board, from engineers designing systems to operators figuring out procedural work-arounds in the field. Empowering those people to improve resiliency involves recognition by senior leaders of the importance of mission assurance and cultural changes that empower our Airmen to make a difference. It is absolutely critical that the Air Force leverage the human war fighter and routinely conduct training in a cyber-contested environment utilizing aggressive red teams that simulate a maneuvering enemy. Many of these exercises will not go well, and collateral damage in nonexercise systems is a known risk. The Air Force must also learn to find and celebrate not those Airmen who score 100 percent on a standardized compliance-based test but those who discover and implement creative approaches that keep the mission going during demanding exercises and inspections. The service has no realistic chance of creating robust mission assurance without routinely and accurately exercising in a cyber-contested environment. Although resiliency is critical to operating successfully within that environment, another component of a strong defense is a force that actively finds and reacts to a maneuvering enemy.

Active Defense

The final component—active defense—contributes a way to discover and respond to advanced persistent threats. Defenders must know their mission space and patrol constantly, looking for small clues that can lead to a hidden enemy. Active defense, one that seeks to find and defeat a sophisticated maneuvering adversary, causes problems for an enemy who tries to stay in systems for a long period of time.

Active defense is an emotionally loaded term that sometimes refers to offensive operations outside a defender's systems. However, the subject of this discussion aligns with defensive cyberspace operations internal defensive measures, defined in Joint Publication 3-12 (R), and remains within the defender's system boundaries.[14] Defensive cyberspace operations response actions, or defensive actions taken outside the defender's system, are important but not part of this discussion.[15] It is also important to note that active defense does not always imply real-time monitoring and maneuver; it may rely on periodic checks for some types of systems for which real-time monitoring is neither practical nor desirable. Active defense is not a new concept, and operators already have implemented it in several key sectors.

More forward-leaning organizations, such as major banks, understand active defense and have switched to a network security monitoring construct that involves active defenders inside the network.[16] The Air Force also currently executes robust active defense on its own traditional IT systems, like NIPR and SIPR. Determining how to extend active defense into cyber physical systems is much more daunting. In the near term, defenders will likely need to protect the traditional IT-based equipment that surrounds and touches a cyber physical system such as Windows-based mission planning or maintenance systems for an aircraft rather than implementing monitoring on the platform itself. In the future, as engineers design and build new cyber physical systems, it will be possible to incorporate some elements of active defense where appropriate. It will not be appropriate in all cases.

To monitor and respond within a Windows- or Linux-based device is relatively simple compared to attempting to execute active defense in a cyber physical system that runs proprietary, unique software (e.g., the avionics suite of an aircraft). One of the greatest obstacles is building a workforce capable of understanding both traditional IT hacking and the proprietary protocols that run avionics or industrial control systems. Engineers must also consider performance effects on current systems. Some cyber physical devices cannot be upgraded easily; neither can they take on the increased processing and data-transmission demands necessary to execute active defense. Another consideration is the added attack surface introduced by monitoring systems. Some very powerful network tools are now available for monitoring and response. The thought of an enemy accessing those tools on a friendly network should send chills down the spine of network defenders and motivate them to defend them vigorously. Once architects mitigate these risks, active defense will include several components.

To implement active defense, architects must create three components: maneuver forces, sensors, and tools. The greatest challenge lies in developing maneuver forces that are trained, equipped, and able to execute active defense successfully. Deep technical skills coupled with creativity and flexibility are in high demand every-

where, but they are exactly what the Air Force needs to build maneuver forces in the cyberspace domain. The service must also develop "hybrids" who not only speak the TCP/IP protocol stack of traditional IT but also have a deep understanding of avionics, industrial control systems, or other control system protocols. Moreover, the Air Force struggles with integrating creativity and flexibility within a strictly hierarchical structure and culture that values compliance and conformity. The service's culture is changing, but it must do so more quickly if we wish to avoid alienating some Airmen who can be our most potent maneuver forces in cyberspace. Finding, developing, and keeping the ones we need is a start, but we must also give them the sensors they need to find a hidden enemy.

A capable sensor suite is the second component of active defense. Cyberspace maneuver forces must be able to find a hidden enemy by following the clues and evidence across networks. Standard intrusion detection systems, part of any competent defense in depth, are a starting point, but the sensors needed by maneuver forces must go further and have more capability. The latter brings greater training requirements for personnel who use sensors because the risk of a negative outcome increases if they do not understand their tools and the effects they can generate on the network. A single overaggressive scan can bring an enterprise network to its knees. It is also worth mentioning that signature-based systems generally will not see advanced, persistent threats. Advanced actors in cyberspace have long been able to write malicious code that current scanners will not find—threats that active defenders should focus on.

The final component is that after cyberspace maneuver forces have located an adversary hiding in their systems, they must have the tools or weapons that allow them to defeat him (i.e., prevent him from fulfilling his objectives). Disruption, denial, and deception are all potential approaches for defenders once they identify an enemy.[17] After such a discovery, creative defenders have an entire universe of ways to exploit him. Furthermore, they do not have to limit themselves to "micro" approaches to whatever code the enemy implanted. The use of software-defined networking permits "macro" approaches that involve changing the entire environment in ways that make it hostile to enemy malware. It is also conceivable for defenders to react on the system level and prioritize what they protect, much like the human body will sacrifice limbs to frostbite to keep the core alive. All of these approaches demand different tool sets that defenders should have developed and ready to utilize immediately.

Moving beyond Theory

Even if the theoretical construct suggested here is correct, it means little unless the Air Force can actually implement it in meaningful ways across the enterprise. The first step is for various communities to comprehend that although their preferred approach to mission assurance is correct, so are the other ones and that all three approaches must work together for maximum effect. An important step was the creation of Task Force Cyber Secure by the Air Force chief of staff with a mandate to look at assurance of the service's five core missions in and through cyber-

space across the entire enterprise. Since the task force was a temporary construct, the challenge now lies in building that enterprise-level view into a new set of structures or an enduring framework. The latter will include elements from the IT, acquisition, and cyberspace operations communities tied together through a governance process and organization. Certainly, these changes at the headquarters level are important, but sweeping cultural change across the Air Force is both more difficult and important.

A self-sustaining, evolving Air Force cyberspace culture of empowered individuals who value cyberspace and know its mission-enabling benefits is the desired end state of our Airmen with regard to the cyberspace domain. As part of the task force, Team Cyber Assure examined issues that affect the cyberspace culture of all Airmen—leaders, service providers, cyber warriors, and users. Some of their recommendations concern growing and developing a cyber-aware workforce, providing strategic communications on cyberspace to the workforce, developing and implementing better cyberspace-oriented strategy and innovation, and recruiting and retaining experts in cyberspace.[18] Moving a culture is not easy and will take time. On a shorter timeline, we can make some changes in how we utilize our cyberspace specialists.

Building up the capability to successfully execute active defense across the core missions will involve shifting some resources. We can reasonably assume that the Air Force will not receive a substantial number of new cyber specialists in the current budgetary environment. If 100 cyberspace Airmen are at a base, how is the base leadership going to utilize them? Right now almost all of them are doing IT work by building and maintaining networks; commanders will need to shift some of them to active defense of those networks. Since the workload in building and maintaining networks will not diminish, leaders must contract out more of that workload, thus shifting money from other priorities. These resource decisions will prove very difficult for the future. Presently, the Air Force is aggressively laying the groundwork for that future by executing multiple pathfinders to experiment and determine the best way for cyberspace professionals to function at the wing level. Leaders should reconsider mission priorities in order to resource appropriately. One of the first things they need to do is identify and grasp the mission impact of their key cyberspace terrain.

To more effectively assure its missions in cyberspace, the Air Force must have a better understanding of the enemy and his missions. Gathering intelligence on an adversary's cyberspace capabilities and intentions is extremely difficult, but intelligence professionals are bringing additional focus and effort to this important area. On the mission side, pathfinders at the wing level are starting their programs by examining and developing their key cyber terrain after appropriate training. The acquisition community is also pursuing multiple mission threads to develop the key cyberspace terrain at the Air Force's core-competency level. All of these initial steps call for further work and development that will help clear a path to a better integrated defense of the service's core missions in and through cyberspace.

Conclusions

The best way to effectively defend both IT-based and cyber physical systems is through a combined approach that includes IT-based defense in depth, resiliency, and active defense of those systems. Cyberspace-reliant systems are essential to mission success for the Air Force in the modern world, and a single approach will not provide the most robust defense possible.

Defense in depth, which represents the initial defense, blocks most attacks—particularly the less sophisticated ones. Without solid, basic IT defenses, too many strikes will get through for resilient systems to handle. Without good defense in depth, active defense will also fail because defenders will be overwhelmed and unable to separate and find sophisticated attackers in the mass of noise.

Resiliency offers assurance by keeping missions functioning despite some enemy success. It prevents adversaries from fulfilling their objectives in attacking friendly systems. No defense will ever be completely effective, so without resiliency, defense in depth is required to meet an impossible standard of catching and stopping every attack at the boundary. Resiliency also makes it much easier for active defenders to find a hidden enemy since the latter must tackle numerous nodes and systems to have an effect; thus, the adversary becomes "noisier" and simpler to locate than if he were able to quietly disrupt a single obscure system that creates complete mission failure.

Active defense finds and responds to sophisticated enemy forces such as advanced, persistent threats. It involves monitoring and responding to adversaries within friendly networks but does not extend beyond them into neutral or enemy networks. Without active defense, the high-level adversaries who slip through our IT-based defense in depth will have unlimited time to examine our systems, discover our resiliency measures, and determine ways to bring down even well-constructed resilient systems. Active defense also provides opportunities to mislead or disrupt an enemy through creatively responding to his attacks and potentially falsifying the effects he produces.

Only if we combine all three approaches can we attain robust mission assurance of the Air Force's core missions in and through cyberspace. Each community has a critical role to play, and each depends on successful implementation of the other categories of cyberspace defense. This combined approach plays to our cultural strengths and experience in joint warfare and can achieve a lasting competitive advantage in and through cyberspace for the United States Air Force. ✪

Notes

1. Engineers designed many systems during the Cold War to prevent an enemy from listening in on communications; cryptography was very common for war-fighting systems. What was unexpected was that an enemy could use communications to alter the functioning of platforms such as tanks, ships, or aircraft.

2. For automobiles see Stephen Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces" (paper presented at USENIX Security Conference, San Francisco, 10–12 August 2011), 3–5, http://www.autosec.org/pubs/cars-usenixsec2011.pdf; or Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, 21 July 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Stuxnet provides a famous example of a weapon

targeting industrial control systems. For an in-depth analysis, see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, [2014]).

3. Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press and Potomac Books, 2009), 465–88.

4. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

5. For a book-length discussion of how response and interaction by adversaries create the paradoxical logic of strategy, see Edward N. Luttwak, *Strategy: The Logic of War and Peace*, rev. and enlarged ed. (Cambridge, MA: Belknap Press of Harvard University Press, 2003).

6. The United States Joint Staff has defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, 5 February 2013, GL-4, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

7. Stuxnet is the best known example of an attack crossing into a well-defended air gap. There are plenty of other examples as well. See P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, [2014]), 63; and Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012): 323–24.

8. Dr. William Young at Air University developed the key cyberspace terrain-analysis methodology in this paragraph. I use it here with his permission.

9. "Operational Technology (OT)," Gartner, accessed 8 September 2016, http://www.gartner.com/it-glossary/operational-technology-ot.

10. Shon Harris, *CISSP All-in-One Exam Guide*, 6th ed. (New York: McGraw Hill, 2013), 768.

11. Department of Homeland Security, Risk Steering Committee, *DHS Risk Lexicon*, 2010 ed. (Washington, DC: Department of Homeland Security, Risk Steering Committee, September 2010), 26, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

12. For a completer discussion of this concept, see Col William D. Bryant, USAF, "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015): 87–107.

13. Luttwak, *Strategy*, 40.

14. JP 3-12 (R), *Cyberspace Operations*, II-2–II-3.

15. Ibid., II-3.

16. Richard Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (San Francisco: No Starch Press, 2013), Kindle location 263, chap. 1.

17. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 79–84.

18. Department of the Air Force, "Task Force Cyber Secure (TFCS) Team Cyber Assure Out Brief / Way Ahead," presentation (Washington, DC: Department of the Air Force, 1 June 2016); and Department of Defense, *Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)* (Washington, DC: Department of Defense, September 2015), http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf.

Col William D. Bryant, USAF

Colonel Bryant (USAFA; MA, American Military University; MA, George Washington University; MSS [Master of Space Systems], Air Force Institute of Technology; MAAS [Master of Airpower Art and Science], School of Advanced Air and Space Studies; MSS [Master of Strategic Studies], Air War College; PhD in Military Strategy, School of Advanced Air and Space Studies) is the deputy director, Task Force Cyber Secure, for the Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, DC. The author of *International Conflict and Cyberspace Superiority: Theory and Practice* (Routledge, 2015), Colonel Bryant is a career fighter pilot, strategist, and planner who has served in numerous operational and staff assignments.