For and from Cyberspace

Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance

Col Matthew M. Hurley, USAF

Thirty years ago, at the dawn of the digital age, the notion of a synthetic, virtual realm where human beings would interact and compete was largely the stuff of science fiction.[1] We thrilled to films like *Tron* and *WarGames*; we shuddered to think that "Skynet" might become self-aware, as foretold in the movie *Terminator*. When the movie was over, however, we rubbed the nightmare out of our eyes and stepped back into the light of the "real" world.

Today, we see cyberspace as more than a flight of sci-fi fancy: we consider it an operational domain, as significant as the four traditional environments of land, sea, air, and space.[2] Yet cyberspace differs obviously from those more familiar, natural domains. How does intelligence, surveillance, and reconnaissance (ISR) apply to this new, dynamic, and artificially crafted environment? What challenges face the

Air Force ISR enterprise as it seeks to understand this novel operational realm? Finally, what should that enterprise do in order to meet the problems and demands inherent in cyberspace? This article addresses each of these fundamental questions in turn.[3]

Defining Cyber Intelligence, Surveillance, and Reconnaissance

Unlike ISR operations in the natural domains, those in cyberspace have yet to be formally defined in joint or service doctrine. Despite wide reference to "CYBINT," its relationship to signals intelligence and open-source intelligence, and even calls to establish more granular disciplines such as "SkypeINT" or "VoIPINT," current thinking on the subject remains immature.[4] As Lt Gen Larry D. James, deputy chief of staff for ISR, remarked in 2011, "We're just starting to think through some of those things from an Air Force perspective."[5] Thus, although the term *cyber ISR* has gained increasing traction within Air Force ISR circles, it has simultaneously drawn queries from elsewhere within the Department of Defense (DOD) and the Air Staff as to its meaning.[6] This article begins by offering a conceptual starting point as a springboard to clarity and future doctrinal refinement.

Perhaps we can best understand cyber ISR through two component activities: ISR *from* cyberspace and ISR *for* cyberspace. ISR from cyber dates back to the first efforts to extract data from adversary networks during the 1980s, and analysts today continue to comb cyberspace for "any information of intelligence value [we] can glean from that domain," according to Lieutenant General James.[7] This includes, for example, foreign news media, chat rooms frequented by threat actors, blogs and video from crisis areas, or commercial imagery, to cite just a few applications. It also incorporates the more familiar concept of computer network exploitation (CNE). After collecting this information in cyberspace, we can use it to support operations in any domain.

For its part, ISR for cyber is perhaps best defined by Air Force Policy Directive 10-17, *Cyberspace Operations*, which tasks Air Force ISR to "ensure [the] ability to provide collaborative analysis, fused intelligence, and cross-domain, integrated, and automated ISR PCPAD (planning and collecting, collection, processing and exploitation, analysis and production, dissemination) capabilities to enable cyberspace operations."[8] This definition suggests the criticality of all-source intelligence during the planning and execution of cyberspace operations. Operating in cyberspace demands more than just ISR from cyber; any intelligence discipline can supply information of crucial intelligence value to cyberspace operations.[9] As noted by Maj Gen Robert P. Otto, commander of the Air Force ISR Agency, "When we say 'ISR for Cyber,' we are referring to the ISR conducted to support Cyberspace superiority"—regardless of the source, method, or medium.[10]

CNE, which some individuals mistakenly equate to cyber ISR, falls neatly within the first mission area—ISR from cyber. Air Force doctrine defines CNE as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[11] More explicitly, CNE is "usually performed through network tools that penetrate adversary systems. . . . Tools used for CNE are similar to those used for computer attack, but configured for intelligence collection rather than system disruption."[12] Both descriptions imply deliberate intrusion into target hardware, software, or related networks.[13] However, they do not incorporate the passive collection of open-source information of potential intelligence value, another important form of ISR from cyber. The latter could include downloading publicly released video of the latest adversary fighter, reading foreign doctrine or military publications, monitoring chat rooms, and a host of other activities that do nothing to—and leave nothing on—a cyber system or network. They do, however, contribute to the essential purpose of ISR—getting the right information to the right decision makers at the right time.

Cyber situational awareness, another ISR-related concept that features prominently in the relevant literature, concerns the perception, discernment, and understanding of who is present and what is occurring within cyberspace, whether friendly, hostile, or anywhere in the gradients.[14] Yet situational awareness writ large is more than ISR, shading into command and control, non-ISR elements of battlespace awareness, and even individual cognition.[15] While ISR is central to situational awareness, therefore, the two should not be conflated. We do not consider environmental monitoring an intelligence-collection discipline, for example, although it is a function of battlespace awareness and involves similarly analytic processes. Nor do we count all human knowledge as "information of intelligence value" even though knowledge presupposes awareness.

Given this starting point for defining and bounding cyber ISR, one must then explore the environment in which we conduct it. As the paragraphs below demonstrate, cyberspace as a domain poses significant issues that we must overcome if we wish to understand it fully and operate within it effectively.

Challenges of Cyberspace

RAND analyst Martin Libicki has identified a trend in American political and strategic thinking. Specifically, when confronted with a new paradigm (such as aerial warfare during World War I or the opening of space to military applications), we generally first react by trying to jam the square peg of game-changing innovation into the round holes of the past. Now that we have declared cyberspace an operational domain, Libicki worries that "we will take our old rules and walk them over." However, he contends that "you cannot do that with cyberspace. You have to think about it from its [own] principles."[16] Certainly, broad and enduring commonalities exist in ISR tradecraft and other military activities across all domains, but Libicki's fundamental point—that we cannot simply rewrite existing doctrine and tactics, techniques, and procedures by inserting *cyber* wherever we find *air* or *space*—warrants

attention. The distinctive nature of cyberspace brings new opportunities as well as new challenges, and these call for novel ways of thinking rather than a perfunctory cookie-cutter solution.[17]

The unique attributes of this newest operational milieu distinguish cyber ISR from complementary activities in the "natural" domains. In the first and most obvious place, cyberspace was created by humans, who continuously modify it; each online click or keystroke by over 2 billion users ripples through cyberspace. "The other domains are natural," observes Gen Michael V. Hayden, USAF, retired, former director of the National Security Agency and the Central Intelligence Agency. "This one is the creation of man. Man can actually change this geography, and *anything* that happens there actually creates a change in someone's *physical* space" (emphasis in original).[18] Cyberspace's man-made origin has resulted in three facets that distinguish it from the relatively consistent natural domains: complexity, adaptability, and rate of change. Granted, nature is complex, nature adapts, and nature changes—but not to the degree and pace that cyberspace does. We can still recognize the same mountains, seas, and stars known to our ancestors. Today's cyberspace, however, bears virtually no similarity to its predecessor of just two decades ago—the length of an individual military career.[19]

Regarding complexity, cyberspace is breathtakingly intricate and maddeningly nonlinear. Everything can be connected to everything else in cyberspace—some 50 billion devices produced to date—while objectively small changes routinely produce effects out of all proportion to their initial scale.[20] Consequently, cyberspace thinking "must consider *the relationship of things*, i.e. the network, and how people have chosen to structure and use the cyberspace domain" (emphasis in original)—no easy task, given the number, instability, unpredictability, and complexity of those relationships.[21]

Cyberspace's inherent adaptability contributes to both its complexity and dynamic nature.[22] It continually changes (through the actions of billions of disparate users) to conditions both within and around cyber-

space, such as new technologies, threats, or policies and laws. Of note, the Internet itself was deliberately designed to facilitate rapid expansion and adaptability to technical innovation.[23] The changes that prompt those adaptations also occur at a rapid pace as new, innovative, and often unanticipated technologies continue to alter the cyber landscape more rapidly than they change any other technical realm.[24] According to a quartet of British observers, "The pace of change can be so abrupt as to render the conventional, action/reaction cycle of strategic evolution out of date before it has begun: it is as if a government operational analyst has been sent to observe the effects in battle of the flintlock musket, only to discover upon arrival that the Maxim gun has been invented."[25]

Cyberspace's dramatic growth contributes to its complexity and adaptability. Unlike the physical domains, which are relatively constant in terms of size, cyberspace is expanding exponentially in every significant respect.[26] By mid-2011, more than 2 trillion transactions had traversed cyberspace, involving 50 trillion gigabytes of data.[27] Fast-forward to 2025, when we can anticipate some 5.5 billion digital denizens, representing 60 percent of the world's projected population. They will use 25 million applications to conduct billions of interactions daily, generating or exchanging 50 trillion gigabytes of data *per day*. The online masses will have roughly 3 billion Internet hosts to choose from, each of which may feature thousands of individual websites.[28] For those people seeking to make sense of cyberspace, its rapid expansion poses a compelling problem.

Traditionally, military planners and practitioners have equated size and distance with similar scales of time: traversing great distances or conquering large areas takes additional time. It took more than a week for convoys to sail from the United States to Great Britain in World War II, for example, and nearly 10 months passed between the time that the Allies landed in Normandy and their crossing of the Rhine. In cyberspace, however, time as traditionally understood in military affairs has become irrelevant.[29] Theoretically, we can deliver a cyber payload

from source to target, from any point to any other on the globe, in less time than it takes an average person to blink. Cyberspace has given us operations at the "speed of byte."[30]

Cyberspace's worldwide pervasiveness, when combined with the speed of cyber effects, confers a new and daunting dimension to the notion of "global reach."[31] Physical cyber nodes inhabit each of the natural domains—in, around, and above every continent and sea. Cyberspace crisscrosses the globe, both drawing people together to an unprecedented degree and giving our foes heretofore unimagined avenues of attack.[32] In the past, war fighters have always enjoyed discrete theaters in which to operate.[33] In cyberspace, however, hostile actions may originate in or be routed through literally any location where an Internet-enabled device can function.[34] Furthermore, cyberspace's global nature has rendered traditional borders between sovereign entities essentially meaningless.[35] Because of a savvy adversary's ability to launch intrusions or attacks across multiple frontiers with near impunity, "Geography is completely irrelevant. So there is no use in determining the geo location of some server where, let's say a denial-of-service attack emerged from because I could just set up this server that I use to launch my attack in the United States. It's not a problem. I can do that. I can use a server in China. I can use a server in Malaysia or in Brunei."[36] The worldwide diffusion and geoambiguity of cyberspace complicate effective ISR, since there are no static physical spaces on which to focus attention—a radical departure from geocentric conceptions of ISR.

Not only nation-state borders but also nation-states themselves have become less relevant in cyberspace. No cyber-enabled nation's government can claim a monopoly of force in this domain, nor can it assert total ownership of the infrastructure vital to military operations.[37] In the first case, the low costs of entry into cyberspace, coupled with the widespread availability of increasingly sophisticated threatware, have presented nonstate actors and even individuals the opportunity to conduct activities formerly the exclusive province of a state's security

apparatus.[38] But now, in cyberspace, actors "do not need to be well educated nor well resourced. . . . They simply need to have intent and the ability to use technology to perpetrate their activity."[39] Additionally, some 90 percent of cyberspace infrastructure is privately owned despite its government-sponsored origins—and despite the fact that our government and armed forces rely heavily on that commercial infrastructure.[40] As a result, in cyberspace "distinctions and divisions between public and private, government and commercial, military and nonmilitary are blurred."[41]

These characteristics of cyberspace contribute to "the most vexing question of all" for ISR professionals: attribution of intrusions and attacks.[42] As Air Force Space Command acknowledges, "The ability to hide the true (originating) source of an attack makes it difficult to identify the attacker. Furthermore, the design of the Internet lends itself to anonymity."[43] One factor that complicates attribution—the large number of online actors—is reflected by the difficulty of trying to uncover an insider threat within the DOD. If each user represented a node and each e-mail message a link, one would have to analyze 755,230,064,000 links between 237,387,616 nodes in a single year—a tally that does not include Internet searches, file accessions, or other types of theoretically observable cyber activity.[44]

Compounding the sheer scale of the potential target set are cyber tools that complicate attribution further. Botnets ranging up to millions of machines, proxy sites dedicated to anonymizing, onion routing, and related techniques all pose intimidating barriers to positive attribution.[45] More fundamentally, the Internet in particular "operates on inherently unauthenticated protocols," meaning that "attribution and non-repudiation collide often with anonymity."[46] Though daunting, attribution is "not impossible," according to Col Daniel Simpson, commander of the 659th ISR Group; "however, you need the work of good, hard analysis by smart ISR professionals."[47] Despite improvements regarding attribution, it "is always going to be more difficult," according

to William J. Lynn III, former deputy secretary of defense. "Missiles come with a return address, cyber attacks do not."[48]

Incomplete or inaccurate attribution also exposes the ISR enterprise to potential violations of law, policy, and constitutional norms. Not only can uncertainty regarding the nature of an intrusion (domestic or foreign; criminal, military, or intelligence) delay attribution while title 10/18/50 authorities are untangled, but also inaccurate or premature attribution may lead to infractions under those authorities.[49] As former FBI director Robert Mueller testified, "At the outset, you do not know whether [a cyber intruder] may be a state actor, a group of individuals operating at the behest of a state actor, or a high-school kid across the street."[50] Proposed solutions to this challenge—such as data sharing among the military, intelligence community, and industry; more aggressive, comprehensive collection to enable proactive defense; or "re-engineering" the Internet to facilitate attribution and geolocation—have drawn the ire of organizations advocating online privacy, civil liberties, and Internet freedom.[51] This article does not purport to be a legal note or discussion.[52] Nevertheless, it is worth noting that we risk finding ourselves "in uncharted waters with regard to cyber law," given the sometimes uncertain boundaries between intelligence and law-enforcement activities in cyberspace.[53]

Way Ahead and Recommendations

Considering the obstacles inherent in cyberspace, the ISR enterprise must make and sustain appropriate investments in ideas, resources, and personnel if it wishes to operate effectively in the newest domain. In the realm of ideas, the first task entails determining how ISR fits into the broader scope of cyber operations. Currently, the Air Force and joint community lack consensus on this point. Most military and national doctrine and policy publications concentrate on offensive and defensive cyber activities; for its part, ISR is generally relegated to a supporting role. For example, in 2010 Air Force Space Command—the core function lead integrator for the Air Force cyber enterprise—

described ISR as a "capability" "necessary" to the "missions" of cyberspace support, cyberspace defense, and cyberspace force application.[54]

Such notions fail to recognize that ISR often *is* the mission. At all other times in the course of cyber operations, it remains both central and essential. Indeed, operations in cyberspace are "soaked in intelligence," and without ISR, cyber operations "would be no better than the proverbial shot in the dark."[55] Lieutenant General James contends that "we don't separate ISR from operations in the air and space domains. In cyberspace, they're even more closely intertwined."[56] Therefore, we need doctrinal, educational, and organizational constructs that forcefully emphasize the centrality and operational nature of cyber ISR—not for its own sake but in recognition of the fact that without it we are functionally deaf and blind, to the detriment of all operations.

To be effective, however, cyber ISR needs much more than institutional emphasis, money, or people. The enterprise must adapt its tradecraft to match the operating environment. In the case of cyberspace, ISR must be globally aware and constantly vigilant, predictive rather than reactive, dynamic and agile, and able to manage exponentially increasing volumes of data. This vision further requires changes in the way we recruit and train cyber ISR professionals, how we employ them to protect civil liberties and privacy, and, indeed, how we integrate cyber ISR into the unified intelligence enterprise.

Predictive ISR and Early Warning

According to observers like Mike McConnell, former director of national intelligence, the current "state of the art" in cyberspace ISR and defense relies on "after-the-fact forensics" to assess damage and identify perpetrators of individual attacks.[57] In the past, we have also relied on perimeter defense and firewalls, but capable foes ultimately will find a way to bypass or breach any "Cyber Maginot Line," however sophisticated.[58] Instead, we need a Cyber Distant Early Warning Line, with attribution and defensive capabilities primed to respond to threats before they can do damage.[59]

To facilitate the earliest possible warning of activity occurring literally in the blink of an eye mandates a more predictive approach based on real-time global awareness of cyber activities and the context in which they occur.[60] Predictive cyber ISR builds upon past experience and emerging trends to identify indications of impending digital mischief, such as preexisting grievances against the United States, an active "patriotic hacker" community, online chatter, new technologies, or adversary doctrine.[61] We must monitor these and other potential tipoffs as part of "a continuous process, leveraging indicators to discover new activity with yet more indicators to leverage."[62]

Agile and Dynamic

Of course, "early" warning is relative. During the Cold War, we assumed that an intercontinental ballistic missile would travel some 30 minutes between launch and impact, but today a cyber strike can flash from Beijing to New York City in 30 milliseconds.[63] Such speed requires degrees of agility and dynamism that seem fantastic, even fanciful in the context of "physical" warfare. According to Dr. Kamal Jabbour of the Air Force Research Laboratory, "cyber agility" entails not only rapid analysis but also "anticipation of future behaviors and effects, and effective real-time provisioning of defensive measures."[64] This, however, demands that the ISR enterprise at least tie for the lead in all things cyber: speed, stealth, flexibility, adaptability, and other factors that have made cyberspace so challenging in the first place.[65] Ongoing scientific and technology initiatives, such as "Cyber Vision 2025," offer a valuable starting point for understanding these issues and devising solutions. Secretary of the Air Force Michael Donley has directed the service's leadership to forge a way forward to realize that vision.

Automation and Visualization

The vast amount of data collected in cyberspace recalls a Chinese proverb: "Absolute light and absolute darkness have the same effect—

we cannot see anything."[66] At present, cyber sensors collect petabytes of data, and collection of yottabytes is not far off.[67] Already, however, the collection outstrips our ability to identify the "nuggets," analyze them, and fashion them into actionable intelligence. Cyber ISR, therefore, "requires the development of algorithms and visualizations capabilities to make activities in the cyber domain intelligible."[68] Technologies that enable automated ISR analysis, operating pictures, and predictive software fall to one side of the equation and correctly demand more intellectual and fiscal attention. No less important, however—and arguably paramount—is the element on the other side of the equal sign: the human variable.

Recruiting and Training

Many of us are so-called digital immigrants. Our first direct experience with integrated circuits involved a 1970s-vintage calculator, a digital watch, or perhaps early video games. Cyberspace and the speed at which it evolves continue to frustrate and sometimes frighten those who stepped off the analog boat—willingly or otherwise—into the digital New World. Our successors, though, are a different breed. Today's recruits may well have had their birth announced via e-mail; they may not remember a single moment when a computer was not within immediate view. These are not your father's Airmen. They are still the best in the world, but "Fly, Fight, and Win" has a different connotation to someone whose idea of warfare derives primarily from nine years of playing "Call of Duty." Yet, potentially, these digital natives represent our biggest assets in the realm of cyberspace. Gen Keith B. Alexander, director of the National Security Agency and commander of US Cyber Command, apparently recognizes this, having recently delivered a recruiting pitch at a convention of self-professed hackers.[69] The requisite human talent is there—and abundant. Once on board, it needs only training in the first-tier standards of cyber operations. But that requires "deep and powerful technical and analytic expertise"—expertise that must continually progress to match the domain's explosive evolution.[70] Although Lieutenant General James contends that cyber ISR training

is improving, the task is not yet complete.[71] Given cyberspace's continuous evolution, further refinement of Air Force specialty code–awarding syllabi; graduate courses; and tailored, adaptive on-the-job training must continue to rank among the top priorities for cyber ISR.

"Normalization" of Cyber ISR

Manpower and training, as well as material and technologies, have recently drawn the attention of multiple high-level initiatives within the DOD and the Air Force, including the Air Force chief scientist's "Cyber Vision 2025" study; the 2012 Air Force Cyber Summit; and the DOD's Cyber Strategic Portfolio Review. Concrete outputs—and, consequently, future cyber ISR capacity—will depend upon the results of these and other deliberations, the fiscal environment, and the continued evolution of cyber threats and opportunities. Conceptually, however, work can and should begin today on "normalizing" cyber ISR. As Lieutenant General James and other Air Force ISR leaders have forcefully maintained, effective ISR must be seamless and domain-agnostic. ISR seeks to deliver timely, relevant, and actionable intelligence to the appropriate decision makers. The location and means of collecting intelligence information are of comparatively little significance to that ultimate objective. In this context, normalization involves dismantling the stovepipes we've erected around All Things Cyber and recognizing that, in the end analysis, the resulting information itself matters to the mission—not the manner or domain in which we acquire it. Nevertheless, in light of the distinctiveness of the cyber domain, the comparative newness of our operations within it, and programmatic practicalities, we still have multiple mental and institutional hurdles to clear before ISR for and from cyber is as readily understood, recognized, and resourced as ISR for and from air or space. Ultimately, this is a question of education and leadership, but before we can teach and lead, we must first understand that cyberspace has come into its own as a domain that presents ISR demands and opportunities in fundamentally the same manner as the other domains. Intelligence for and from space was also new and conceptually compartmentalized in the

not-so-distant past, but its contribution to operational effectiveness has grown dramatically with its diminishing novelty.

Protection of Civil Liberties and Privacy

Any and all cyber ISR investments, however, must adhere to the government's obligation to protect civil liberties and constitutional rights.[72] Colonel Simpson acknowledges that "the current infancy of cyber law and policy creates difficulties for ISR in determining and managing authorities and boundaries."[73] The balance among awareness, security, and civil liberties is an evolving one that demands constant attention and carries considerable implications for public trust.[74] This is more than an ancillary concern to the ISR enterprise; as military professionals serving our citizens and Constitution, these issues warrant continued vigilance and strict adherence. Despite today's legal ambiguities that cloud cyberspace and regardless of whatever relevant court decisions appear in the future, the entire intelligence community must remain steadfastly committed to the Constitution and every citizen's right to privacy.

Conclusion

Over the past century, the Air Force and its predecessors have demonstrated their mastery of new operational domains—first in the air and later in space. In both cases, ISR proved critical to opening and securing new environments. Cyberspace, for all its unique attributes, shares that fundamental trait: the absence of timely, relevant, and actionable ISR reduces the success of all other military activities to chance. As the odds stack up against the defender in this new domain, though, relying on chance is not an option.[75] The difficulties facing cyber ISR sometimes seem insoluble, but they only appear that way. No doubt the unprecedented speed of airpower caused considerable mental dislocation during its maturation, as did the vastness of space in the following decades. Without question, as we enter a new operating

environment, we will encounter many of the same intellectual growing pains. We should remain confident, however, in our ability to overcome them through an increasingly persistent and pervasive understanding of cyberspace provided by—and contributing to—cyber ISR. To continue that positive trend, we must invest; to invest, we must commit; but to commit, we must first fully understand the nature and extent of the challenges and opportunities facing us as an Air Force and a nation. ISR is the key to that understanding—in cyberspace as in every other domain of human enterprise. ✪

Notes

1. In *Neuromancer*, William Gibson prophetically coined the term *cyberspace* to hypothesize a flight of science-fiction fancy, "a consensual hallucination experienced daily by billions. . . . Data abstracted from the banks of every computer in the human system. Unthinkable complexity." William Gibson, *Neuromancer* (New York: Ace Books, 1984), 69.

2. Joint doctrine defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 August 2012), 77, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. The author, however, is compelled to agree that "'Cyber' itself is such a nebulous concept that determining the fundamentals of what it is and how it affects the military domain has exercised years of planning man-hours." Daniel Wasserbly, "Charting the Course through Virtual Enemy Territory," *Jane's International Defence Review* 44, no. 5 (May 2011): 60. Or, as Gen Michael V. Hayden, USAF, retired, observed, "Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon." Michael V. Hayden, "The Future of Things 'Cyber,' " *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 3, http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.

3. This article does not address threats—the literature regarding that subject is as expansive and varied as the threats themselves. However, in all military operations, effective threat response begins with conceptually sound, well-planned, and well-executed ISR.

4. For CYBINT see Dr. Kamal T. Jabbour, *50 Cyber Questions Every Airman Can Answer* (Wright-Patterson AFB, OH: Air Force Research Laboratory, 7 May 2008), 20, http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf; for CYBINT's relationship to signals intelligence, see, for example, Air Force Doctrine Document (AFDD) 2-0, *Global Integrated Intelligence, Surveillance, & Reconnaissance Operations*, 6 January 2012, 40, http://www.e-publishing.af.mil/shared/media/epubs/afdd2-0.pdf; and for open-source intelligence as described by Frederick J. Wettering, see "The Internet and the Spy Business," *International*

Journal of Intelligence and Counterintelligence 14, no. 3 (Fall 2001): 344. See also "Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012–2025," draft, AF/ST TR 12-01, 1 September 2012, 42. "VoIP" refers to Voice over Internet Protocol applications.

5. Ben Iannotta, "Voice for Balance," *DefenseNews*, 1 November 2011, http://www.defensenews.com/article/20111101/C4ISR01/111010318/Voice-balance.

6. As the author has personally experienced multiple times within the past few months, as of the time of this writing.

7. Lt Gen Larry D. James, interview by the author, 30 July 2012.

8. Air Force Policy Directive 10-17, *Cyberspace Operations*, 31 July 2012, 3, http://www.e-publishing.af.mil/shared/media/epubs/AFPD10-17.pdf.

9. Intelligence and National Security Alliance, *Cyber Intelligence: Setting the Landscape for an Emerging Discipline* (Arlington, VA: Intelligence and National Security Alliance, September 2011), 14, https://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/Sept_ISOAG_CyberIntel.pdf. See also AFDD 3-12, *Cyberspace Operations*, 15 July 2010, 24, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf, which notes that "employing full-spectrum cyber effects requires a multi-INT analysis approach" and "all-source cyber-focused ISR."

10. Maj Gen Robert P. Otto, written interview responses, 14 August 2012.

11. AFDD 3-12, *Cyberspace Operations*, 49.

12. Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, CRS Report for Congress (Washington, DC: Congressional Research Service, 20 March 2007), 5, http://www.au.af.mil/au/awc/awcgate/crs/rl31787.pdf.

13. Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrop Grumman Corporation, 9 October 2009), 8–9, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

14. Dr. Kamal Jabbour, "The Science and Technology of Cyber Operations," *High Frontier* 5, no. 3 (May 2009): 11, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf; "Cyber Vision 2025," 20; Air Force Space Command, *Functional Concept for Cyberspace Operations* (Peterson AFB, CO: Air Force Space Command, 14 June 2010), 7; and Lt Gen Michael J. Basla, "Cyberspace from a Service Component Perspective" (address, Cyberspace Symposium, US Strategic Command, 15 November 2011), http://www.afspc.af.mil/library/speeches/speech.asp?id=686. In his address, Lieutenant General Basla, vice-commander of Air Force Space Command, described cyber situational awareness as "an operationally relevant picture of the battlespace to include the status of the joint networks, of the Air Force networks, and the disposition of our forces, friendly or otherwise."

15. The *Manual for the Operation of the Joint Capabilities Integration and Development System* (Washington, DC: Joint Staff J8 / Joint Capabilities Division, Pentagon, 19 January 2012), https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=1517681, defines the joint capability area "battlespace awareness" as "the ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision making by leveraging all sources of information to include Intelligence, Surveillance, Reconnaissance, Meteorological, and Oceanographic" (B-B-2). The individual cognitive aspects of situational awareness are perhaps best exemplified by the single-seat-fighter-pilot origin

of John Boyd's observe, orient, decide, act (OODA) loop. See, for example, Col Phillip S. Meilinger, ed., *The Paths of Heaven: The Evolution of Airpower Theory* (Maxwell AFB, AL: Air University Press, 1997), xxiii; and Maj David S. Fadok, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis" (Maxwell AFB, AL: School of Advanced Airpower Studies, 1995), 13.

16. Martin Libicki, "Cyberpower and Strategy" (remarks at the 8th International Institute for Strategic Studies Global Strategic Review, "Global Security Governance and the Emerging Distribution of Power," Sixth Plenary Session, 12 September 2010), [3], http://www.iiss.org/EasySiteWeb/getresource.axd?AssetID=46892&type=full&servicetype=Attachment.

17. Lt Col Steven E. Cahanin, USAF, "Principles of War for Cyberspace," research report (Maxwell AFB, AL: Air War College, Air University, 15 January 2011), 1, http://www.airpower.au.af.mil/digital/pdf/articles/Jan-Feb-2012/Research-Cahanin.pdf.

18. Hayden, "Future of Things 'Cyber,' " 4.

19. Comparing today's cyberspace to its early 1990s incarnation, for example, one might see similarities in standards such as e-mail, message boards, and online connectivity to informational databases. Radical changes such as the ubiquity of social media, streaming video, online voice and video communications, mobile connectivity, and, yes, the sophistication and pervasiveness of today's cyber threat have all, in retrospect, far outdistanced even the most ambitious forecasts of 20 years ago.

20. Cahanin, "Principles of War for Cyberspace," 2; Brookings Institution, *Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch* (Washington, DC: Brookings Institution, 20 September 2011), 2, http://www.brookings.edu/~/media/events/2011/9/20%20cyberspace%20deterrence/20110920_cyber_defense.pdf; and Paul W. Phister Jr., "Cyberspace: The Ultimate Complex Adaptive System," *International C2 Journal* 4, no. 2 (2010–11): 13–14.

21. Cahanin, "Principles of War for Cyberspace," 2.

22. "Remarks of the Honorable Michael B. Donley, Secretary of the Air Force, Air Force Association CyberFutures Conference, Gaylord National Resort, Friday, March 23, 2012," 3, http://www.af.mil/shared/media/document/AFD-120326-056.pdf.

23. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 2, http://www.defense.gov/news/d20110714cyber.pdf.

24. Cahanin, "Principles of War for Cyberspace," 3–4.

25. Paul Cornish et al., *On Cyber Warfare*, Chatham House Report (London: Chatham House [Royal Institute of International Affairs], November 2010), 29, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.

26. Even though space may be infinite, or finite but expanding, or finite and contracting (theories vary), the human dimension of space—that is, where humans have established a more-or-less permanent presence, even remotely—is almost exclusively confined to our own solar system. With the exception of the Apollo moon landings and interplanetary, lunar, or solar probes, this human dimension resides between 50 and 22,000 miles above the earth's surface.

27. Brookings Institution, *Deterrence in Cyberspace*, 2. By mid-2012, every minute of every day saw the following uploaded to or traversing through cyberspace: 48 hours of Youtube video; 204,166,667 e-mail messages; 2,000,000 Google search queries; 684,478 Facebook

posts; 571 new Internet websites; 27,778 *Tumblr* blog posts; and more than 100,000 Twitter tweets. Oliur Rahman, "How Much Data Is Created on the Internet Every Minute?," *Ultralinx*, 24 June 2012, http://theultralinx.com/2012/06/data-created-internet-minute.html.

28. "Cyber Vision 2025," 9.

29. Richard M. Crowell, *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare* (Newport, RI: Naval War College, 2010), 21, http://www.carlisle.army.mil/DIME/documents/War%20in%20the%20Information%20Age%20-%20A%20Primer%20for%20Cyberspace%20Operations%20in%2021st%20Century%20Warfare%20-%20R%20M%20%20Crowell.pdf.

30. Contrary to popular belief, activities in cyberspace do not occur at the speed of light; rather, cyber operates at the speed of electrons. Light travels at approximately 186,000 miles per second, while electrons—due to the fact that they have mass—travel "only" two-thirds of that speed—some 125,000 miles per second. Jabbour, *50 Cyber Questions*, 11.

31. As suggested by Mike McConnell, "Cyber Insecurities: The 21st Century Threatscape," in *America's Cyber Future: Security and Prosperity in the Information Age*, vol. 2, ed. Kristin M. Lord and Travis Sharp (Washington, DC: Center for a New American Security, June 2011), 25–39, http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf.

32. Robin Geiß, "The Conduct of Hostilities in and via Cyberspace," *Proceedings of the Annual Meeting* (American Society of International Law) 104 (24–27 March 2010): 371; and Crowell, *War in the Information Age*, 21.

33. Even the world wars weren't, strictly speaking, for Allied commanders didn't have to worry about that potential Axis thrust from Switzerland or Swaziland.

34. Geiß, "Conduct of Hostilities," 371; and Cahanin, "Principles of War for Cyberspace," 5.

35. Susan Freiwald, "Electronic Surveillance at the Virtual Border," *Mississippi Law Journal* 78, no. 2 (Winter 2008): 329, http://www.olemiss.edu/depts/ncjrl/pdf/ljournal09Freiwald.pdf; Geiß, "Conduct of Hostilities," 371; and Cahanin, "Principles of War for Cyberspace," 5.

36. Brookings Institution, *Deterrence in Cyberspace*, 15; and Crowell, *War in the Information Age*, 21.

37. Cyber "bases," cyber "airspace," or cyber "force structure," for example.

38. McConnell, "Cyber Insecurities," 61; Gregory C. Radabaugh, "The Evolving Cyberspace Threat" (working paper, Air Force Intelligence, Surveillance, and Reconnaissance Agency, August 2012), 8; Cornish et al., *On Cyber Warfare*, 30; and Crowell, *War in the Information Age*, 21.

39. Intelligence and National Security Alliance, *Cyber Intelligence*, 7. For similar assessments, see Kevin Coleman and John Reed, "Cyber Intelligence," DefenseTech.org, 3 January 2011, http://defensetech.org/2011/01/03/cyber-intelligence/.

40. Cahanin, "Principles of War for Cyberspace," 5.

41. House, *House Armed Services Subcommittee, Cyberspace Operations Testimony, General Keith Alexander, Washington, D.C., Sept. 23, 2010*, [1], 111th Cong., 2nd sess., http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf. Rep. Ike Skelton (D-MO), chairman of the House Armed Services Committee at the time, made this statement in his introductory remarks.

42. Kenneth Geers, *Sun Tzu and Cyber War* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 9 February 2011), [4], http://www.ccdcoe.org/articles/2011/Geers

_SunTzuandCyberWar.pdf. For a more thorough treatment of the attribution challenge, see Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

43. Air Force Space Command, *Functional Concept for Cyberspace Operations*, 10.

44. Rand Waltzman, "Anomaly Detection at Multiple Scales" (presentation, DARPA Cyber Colloquium, Arlington, VA, 7 November 2011), slides 3–4.

45. "Onion routing" refers to a technique, originally developed by the Navy, to hide the origin and content of packets as they traverse a network. Packets are sent through a network of randomly selected proxy servers, with successive levels of encryption and then decryption, before delivery to their final destination as plain text. W. Earl Boebert, "A Survey of Challenges in Attribution," in National Research Council of the National Academies, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010), 43–46.

46. Jabbour, *50 Cyber Questions*, 9.

47. Col Daniel Simpson, commander, 659th ISR Group, interview by the author, 8 August 2012. The 659th is the Air Force's premier cyber ISR unit, focused on "digital network exploitation analysis and digital network intelligence." See Capt Karoline Scott, "New ISR Group Supports Cyber Operations," Air Force News Service, 10 September 2010, http://www.af.mil/news/story.asp?id=123221324; and AFDD 3-12, *Cyberspace Operations*, 24.

48. Kristin Quinn, Vago Muradian, and Marcus Weisgerber, "The Pentagon's New Cyber Strategy," *DefenseNews*, 18 August 2011, http://www.defensenews.com/apps/pbcs.dll/article?AID=2011108180316.

49. Libicki, *Cyberdeterrence and Cyberwar*, 96.

50. Wasserbly, "Charting the Course," 60.

51. Decian McCullagh, "House Passes CISPA Internet Surveillance Bill," ZDNet, 27 April 2012, http://www.zdnet.com/news/house-passes-cispa-internet-surveillance-bill/6360341. One opposing representative, Jared Polis (D-CO), claimed that the Computer Intelligence Sharing and Protection Act (CISPA) would "waive every single privacy law ever enacted in the name of cybersecurity. . . . Allowing the military and NSA to spy on Americans on American soil goes against every principle this country was founded on." See also Sanjay Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence," *Communications of the ACM* 54, no. 8 (August 2011): 137; and Mike McConnell, "Mike McConnell on How to Win the Cyber-War We're Losing," *Washington Post*, 28 February 2010, B01, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. In addition to general rights-oriented organizations such as the American Civil Liberties Union, advocacy groups include the Electronic Frontier Foundation (which offers a tutorial on "Surveillance Self-Defense" at https://ssd/eff/org), savetheinternet.com (which features the "Declaration of Internet Freedom"), the Electronic Privacy Information Center, the Center for Democracy and Technology, the Technology Liberation Front, and the OpenNet Initiative ("Our aim is to investigate, expose and analyze Internet filtering and surveillance practices"), http://opennet.net/about-oni. In the author's opinion and experience, no category of activity by the intelligence community has drawn such keen attention and public backlash in the United States since the Church Committee reports of 1976.

52. For insight into recent legal debates regarding cyberspace privacy, search and seizure law, and other constitutional norms, see Susan W. Brenner, "Fourth Amendment Future:

Remote Computer Searches and the Use of Virtual Force," *Mississippi Law Journal* 81, no. 5 (2012): 1229–62; Timothy Casey, "Electronic Surveillance and the Right to Be Secure," *University of California–Davis Law Review* 41, no. 3 (February 2008): 977–1033; Elizabeth Gillingham Daly, "Beyond 'Persons, Houses, Papers, and Effects': Rewriting the Fourth Amendment for National Security Surveillance," *Lewis & Clark Law Review* 10, no. 3 (Fall 2006): 641–71; Dan Fenske, "All Enemies, Foreign and Domestic: Erasing the Distinction between Foreign and Domestic Intelligence Gathering under the Fourth Amendment," *Northwestern University Law Review* 102, no. 1 (2005): 343–81; Freiwald, "Electronic Surveillance," 329–62; John N. Greer, "Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and Protection of Privacy Rights and Civil Liberties in Cyberspace," *Journal of National Security Law and Policy* 4, no. 1 (2010): 139–54; Orin S. Kerr, "Applying the Fourth Amendment to the Internet: A General Approach," *Stanford Law Review* 62, no. 4 (April 2010): 1005–49; Mike McNerney, "*Warshak*: A Test Case for the Intersection of Law Enforcement and Cyber Security," *University of Illinois Journal of Law, Technology and Policy* 2010, no. 2 (Fall 2010): 345–57; Amanda Yellon, "The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications," *Journal of Business & Technology Law* 4, no. 2 (2009): 411–37; and Mark D. Young, "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security," *Stanford Law & Policy Review* 22, no. 1 (2011): 11–39. Representative questions raised by these notes and case studies include the following:

- Are computers analogous to "containers" protected from "unreasonable search and seizure" under the Fourth Amendment?
- Is online communication to be treated the same as sealed letters under privacy and constitutional rights (content vs. noncontent)?
- Is surveillance of a specific individual's cyber communications (particularly e-mail and texts, for which an expectation of privacy exists) subject to the same limitations and restrictions as wiretapping?
- How do cyber intelligence professionals ensure compliance with mandates of Executive Order 12333, United States Intelligence Activities, to limit collection against foreign threats (i.e., how can you tell if the subject under surveillance or collection is or is not a "US person" subject to constitutional and executive protections)?
- Above all, how are individual rights to be balanced against the government's responsibility to ensure collective security against foreign *and* domestic threats?

53. McNerney, "*Warshak*," 346.
54. Air Force Space Command, *Functional Concept for Cyberspace Operations*, 15.
55. Libicki, *Cyberdeterrence and Cyberwar*, 155, 156.
56. James, interview.
57. RADM J. Michael McConnell, telephone interview by the author, 23 August 2012.
58. See, for example, William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September–October 2010): 99.
59. Ned Moran, "A Cyber Early Warning Model," in Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010), 200; and Geers, *Sun Tzu and Cyber War*, 10.

60. Gregory C. Radabaugh, "The Evolving Cyberspace Threat" (working paper, Air Force Intelligence, Surveillance, and Reconnaissance Agency, August 2012), 9.

61. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (paper presented at the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, 17–18 March 2011), 3, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf; Moran, "Cyber Early Warning Model," 208; and Radabaugh, "Evolving Cyberspace Threat," 9.

62. Hutchins, Cloppert, and Amin, "Intelligence-Driven Computer Network Defense," 3.

63. McConnell, telephone interview.

64. Dr. Kamal Jabbour, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly* 4, no. 1 (Spring 2010): 65, http://www.au.af.mil/au/ssq/2010/spring/spring10.pdf.

65. Little wonder that some of our Air Force cyber warriors unofficially refer to themselves as "ninjas."

66. Richard Stiennon, *Surviving Cyberwar* (Lanham, MD: Government Institutes, 2010), 121.

67. A petabyte is 1 billion gigabytes; a yottabyte is 1 billion petabytes.

68. "Cyber Vision 2025," 40.

69. Damon Poeter, "DefCon: NSA Boss Asks Hackers to Join the Dark Side," *PC Magazine*, 29 July 2012, http://www.pcmag.com/article2/0,2817,2407783,00.asp.

70. Intelligence and National Security Alliance, *Cyber Intelligence*, 14. See also Wayne Michael Hall and Gary Citrenbaum, *Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments* (Santa Barbara, CA: Praeger, 2012).

71. James, interview. As Colonel Simpson observes, "Training is another challenge to overcome," given "the current lack of technical ability to conduct detailed cyber analysis." Simpson, interview.

72. Lynn, "Defending a New Domain," 103.

73. Simpson, interview.

74. A 2010 survey, for example, found that 88 percent of Americans believe they should enjoy the same legal privacy protections online as they do in the physical sphere. Only 4 percent disagreed. US Department of Commerce, *Comments of Digital Due Process, in the Matter of Information Privacy and Innovation in the Internet Economy*, docket no. 1004020174-0175-01 (Washington, DC: US Department of Commerce, National Telecommunications and Information Administration, 14 June 2010), 4, http://www.digitaldueprocess.org/files/NTIA_NOI_061410.pdf.

75. Lynn, "Defending a New Domain," 99.

Col Matthew M. Hurley, USAF

Colonel Hurley (USAFA; MA, University of Washington; MAAS, Air University; PhD, Ohio State University) is the director of doctrine and policy integration for the Office of the Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (ISR), Headquarters US Air Force, Pentagon, Washington, DC. In this capacity, he ensures that Air Force ISR equities and best practices are appropriately codified in allied, joint, and Air Force doctrine and policy documents. A career intelligence officer, Colonel Hurley has previously served in assignments supporting Air Mobility Command, US Forces Korea, US Air Forces in Europe, and Allied Air Forces Central / Northern Europe, including contingency deployments to Southwest Asia and the Horn of Africa. He is a past winner of the Ira C. Eaker Award and received the 1989 Air Force Historical Foundation Award for research of historical significance to the Air Force. His most recent work, *On the Fly: Israeli Airpower against the Al-Aqsa Intifada, 2000–2005*, was published by the Air Force Research Institute, Maxwell AFB, Alabama, in 2010.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

http://www.airpower.au.af.mil