Winter 2017

Brandishing Our Air, Space, and Cyber Swords: Recommendations for Deterrence and Beyond

Mark Reith
Air Force Institute of Technology

Brandishing Our Air, Space, and Cyber Swords

Recommendations for Deterrence and Beyond

Lt Col Mark Reith, USAF, PhD*

Courtesy Stacy Burns

The United States has arrived at a historic crossroads for space and cyber. For decades, space and cyber have been treated as neutral territory or part of a global commons, but the rise of competitors and the commoditizing of technology within these domains have drastically changed the calculus of strategic deterrence. One road takes the United States down the path of massive and time-intensive investments into hardened and resilient systems with no guarantee that next-generation technology will be any more resistant to crafty attackers than the last.

Another road takes the United States down the path of multidomain offensive capabilities to create multiple dilemmas that overwhelm and hold the adversary at

*Special thanks to Col Brad Pyburn, Col David Snoddy, Col Heather Blackwell, Lt Col Eric Trias, Lt Col Joy Kaczor, and Capt Carlos Rodriguez for their insightful contributions.

risk, but the efficacy of this approach across a range of actors is unknown. Yet just beyond the technical horizon, we face the implications of science fiction in motion as new technologies such as artificial intelligence, robotics, and weaponized lasers are developed and fielded against a disturbing backdrop of world events.[1] Consider the Russian–Ukrainian cyber conflict playing out across the fabric of society, including utilities, mass media, and finance, and all while the international community fails to establish intervention redlines as malware spills beyond the borders of the conflict.[2]

> *Strategic deterrence in the 21st century is much bigger than nuclear deterrence was in the 20th century. The US military is still "catching up" to this new deterrence reality and having a robust discussion on what deterrence means in today's global threat landscape.*
>
> —Gen John Hyten, USAF
> Commander, US Strategic Command

> *Conflict may occur along the spectrum at any point, in varying degrees of intensity, with more than one adversary, and in multiple domains. At all phases. . . our planning and operations are designed to deter and develop "off ramps" to de-escalate the conflict. . . while dissuading our adversaries from considering the use of cyber attacks, counterspace activities, or nuclear weapons.*
>
> —Adm Cecil D. Haney, USN
> Former Commander, US Strategic Command

Furthermore, ponder North Korea's offset strategy to hold conventional American forces at risk with nuclear weapons while employing asymmetrical tools with a clear intent and resolve to challenge US hegemony.[3] As we grapple with this dynamic environment, we find ourselves at the precipice of the next revolution in military affairs, and our next investments will heavily influence our future options.

This article examines how the nation could better prepare to deter aggressive action in space and cyberspace, and if necessary, prevail should deterrence fail. The key themes throughout this article include a strong need for space and cyber situational awareness, the need for an international attribution and escalation framework, and a national investment in space and cyber education, along with an updated national strategy and military doctrine. Although related, this article focuses on deterrence and avoids the topic of cyber coercion.

Problematic Assumptions in the Strategic Deterrence Framework

> *Deterrence prevents adversary action through the presentation of a credible threat of counteraction. In both peace and war, the Armed Forces of the United States help to deter adversaries from using violence to reach their aims. Deterrence stems from an adversary's belief that a credible threat of retaliation exists, the contemplated action cannot succeed, or the costs outweigh the perceived benefits of acting. Thus, a potential aggressor chooses not to act for fear of failure, cost, or consequences.*
>
> —Joint Publication 3-0, *Joint Operations*

The concept of deterrence has a long history in warfare and military doctrine reflects a deep understanding of its most salient elements. From the Joint Publication's description of deterrence, the most important element involves the adversary's belief in retaliation, failure, or unacceptable costs. The description makes several assumptions that are problematic when considering space and cyberspace. The first assumption asserts that the United States can quickly and reliably attribute behavior to an adversary. The second assumption is that the adversary can observe success or failure of their actions, let alone the actions of others. Finally, the third assumption states that costs and benefits can be measured and rationalized. Challenging these assumptions may reveal opportunities to exploit situations.

For deterrence to be effective, several conditions should be met:

1. *The threat must be communicated accurately to the target.*
2. *The target must clearly understand the threat.*
3. *The target must believe that the anticipated cost of its undertaking the action outweighs potential benefits.*
4. *The target must believe that the "deterrer" will take the threatened action(s).*

—USAF Doctrine Annex 3-0
Operations and Planning

The US Air Force elaborates on the conditions of deterrence as part of USAF doctrine. Here, too, we observe assumptions that are problematic in the modern age. First, cyber and space activities are often hidden due to the highly classified nature before and after they have occurred, and often under the guise of anonymity. Unlike nuclear tests and operations that are generally observable to all adversaries, cyber and space activities may or may not be detectable by the target, and typically not by third parties. Second, the description assumes that all adversaries are paying attention and understand the threat. Within the space and cyber domains, this may require specialized tools that detect disturbances in these domains, and more importantly, interpret correctly for their situation. Finally, the description assumes that the prep work supporting threatening actions has already been accomplished. For example, the United States has strong relations with the international community and generally adheres to an ethical and legal framework to maintain the legitimacy of its world leadership role. An adversary, suspecting that no legal framework for retaliating across the global commons exists, might not believe the United States is willing to take threatening actions. Additionally, the same adversary might not believe that the United States has prepositioned space and cyber weapons available to retaliate. Although not addressed in Joint or USAF Doctrine, the timing of retaliatory action must also be considered. Space and cyber attacks have the potential to rapidly scale and affect large populations, then disappear into the complexity of cyberspace. This highlights the need for agile options, to include real time action, lest aggressors become emboldened with guerrilla style tactics.

Challenges in Deterring Cyber Attacks

Summary of Challenges to Cyber Deterrence

- *Difficulty of attributing cyber attacks to their perpetrators*
- *Ease of acquiring cyber weapons and conducting cyber attacks*
- *Broad scope of state and nonstate actors who engage in cyber attacks for a multitude of reasons and against both state and nonstate targets*
- *Short shelf life of many cyber weapons*
- *Difficulty of establishing thresholds and red lines for cyber aggression*
- *Difficulty of setting and enforcing international norms regarding cyber behavior*
- *Challenges associated with avoiding escalation*

—Dorothy E. Denning
Emeritus Distinguished Professor
Navy Postgraduate School

Some scholars have identified a collection of challenges associated with cyber deterrence.[4] Information security researcher Dorothy E. Denning summarizes many of these challenges and compares, as many others have, the nature of cyber deterrence to that of nuclear deterrence. Key differences might include the degree of difficulty in acquiring weapons, the shelf life of these weapons, and the motivations and attribution of firing these weapons, to name a few. One might infer from the community of researchers that instead of comparing cyber deterrence to nuclear deterrence, strategists and policymakers need to instead reflect on the strategic deterrence framework and either shape space and cyber to allow the traditional deterrence model to work or reset expectations about the effectiveness of deterrence in these domains. The next section provides some perspectives on how to accomplish both.

Applying the Deterrence Framework to Cyber

Deterrence is all about capability and intent, and in cyber we've shown a little of either publicly. I think of the nuclear "tests" we conducted in the '50s/'60s to demonstrate not just capability, but resolve. . . we should showcase the broad spectrum of capabilities we can bring to bear through our powerful "engine" of offensive cyber. We show "demonstrations" of how cyber can impact kinetic systems—this will also help decision makers properly prioritize cyber security/hygiene/defense through the proper risk-informed investment strategies.

—Col Brad Pyburn, USAF
Commander, 67th Cyberspace Wing

As previously discussed, applying the deterrence framework to the cyber domain can be challenging and complicated. This article expands upon Geist's recommendation for a "Strategy of Technology" to implement a cyber deterrence framework.[5] Geist outlines three components of his strategy: denial, resilience, and offensive capabilities. The article examines each component, maps it back to DOD Joint Operations

doctrine, outlines shortfalls, and makes recommendations for building a robust deterrence framework.

Deterrence by Denial (Fear of Failure)

The first, and generally considered the most effective, component is deterrence by denial. This type of deterrence is characterized by rendering cyber weapons ineffective such that an adversary is discouraged to even attempt an attack. From DOD Joint Operations, this exploits a fear of failure and opens the possibility of potential attribution. The classic example involves a strong vulnerability patching approach that leaves exploit weapons inert. Denial works because exploits tend to be fragile in that some technical and situational conditions need to be satisfied before the exploit is effective. The fact that some conditions exist gives great hope as a form of deterrence because the defender can often influence many of these conditions. The typical problem involves a numbers game: multiply the number of potential vulnerabilities (order of thousands) with the number of enterprise systems (order of hundreds of thousands) and the number of exploit attempts (that is, the Air Force blocked 1.3 billion connection attempts in 2016), and you get an upper bound on the number of possible exploits in a given time frame.[6] Granted that actual risk exposure is dependent on linkages between systems, vulnerabilities, and exploit attempts, but the key theme involves a scale of problem that is difficult to manage. Another typical problem involves some legacy systems from developers who never imagined these systems would be exposed to exploit attempts. Utility infrastructure, vehicles, and embedded systems are good examples of such exposure.

The United States can enhance its deterrence by denial strategy in several ways. First, the most obvious solution involves implementing cyber security best practices such as defense in-depth, patching, configuration management, strong authentication, deep inspection of communications traffic, and so on. Chinese research into quantum cryptography using satellites is a great example of strategic investment into their denial deterrence.[7] Second, workforce education and training are paramount, along with exercises, drills, and accountability for online behavior. Third, the United States needs to change expectations regarding technology. Specifically, strategists and policymakers need to stop viewing information technology as a utility, and instead expect a perpetually contested environment. In doing so, they can segment forces into groups with extremely limited exposure to cyber threats, accepting the potential for a reduced capability for the short period in which the cyber terrain is contested.

Deterrence by Resiliency (Cost)

The second component is deterrence by resiliency. This type of deterrence is characterized by increasingly expensive efforts such that an adversary is discouraged, although not necessarily prevented, from attacking. From DOD Joint Operations, this exploits a resource cost in multiple ways. First, this strategy may consume the adversary's exploit tools and zero-day opportunities. Exploit owners cannot guarantee sole ownership, and over time such tools and opportunities often become stale. Once an exploit is understood, and a patch is deployed, the tool may have reduced

value. This is particularly a problem if the exploit tool was expensive to develop or acquire. Loss of anonymity is a related cost because as the exploit tool or technique is repeatedly used, the defender may piece together enough information for reasonable attribution. Second, as the defender's capacity increases, the adversary may require a larger force to find and exploit vulnerabilities *that meet their specific objectives*. Consider how redundancies may dampen the effect of denial of service attacks while increasing the adversary's required resources. Third, over time previously understood networks may change, reducing the value of reconnaissance info and prompting rework. Finally, even upon successful exploit, active defenders might detect and force an adversary out, thus inducing the cost of finding another way back into the system.

The United States can enhance its deterrence by resiliency strategy in several ways. First, the most straightforward approach involves investment into active defense capabilities. Additional manpower and research into automated detection and investigation capabilities help find, fix, track, engage, and assess adversaries on contested US networks. Investments into mission mapping technology help defenders identify key cyber terrain and fight adversary activity to assure missions.[8] Second, leverage the natural advantage of the home game. Since cyberspace is malleable and mutable, shaping the environment to give defenders the advantage makes sense. Deploy software-defined networks to unpredictably change the environment and render previous adversary reconnaissance useless. Harness the workforce by defining meaningful cyber conditions based on mission set rather than by geography, and exercise such conditions routinely. Third, leverage the natural complexity inherent in cyberspace. Deploy thousands of decoy systems, and let adversaries run around the mirror maze while defenders observe and learn from their tactics. Deploy distributed file systems that store fragments of files across thousands of systems. Owners will be able to find and reassemble, whereas adversaries will grow frustrated and make mistakes, ultimately leading to attribution. Planting malware in these decoys and file systems may ultimately increase the adversary's cost considerably. Furthermore, revealing evidence of a cyber attack to the international community, particularly in the context of standing treaties, may also increase an adversary's cost.

Deterrence by Punishment (Consequences)

Finally, the third component is deterrence by punishment. This type of deterrence is characterized by attacking, or threatening to attack, the adversary directly such that they are too intimidated to fight back. From DOD Joint Operations, this exploits a fear of consequences but requires strong attribution to be effective. Punishment deterrence can be a complex topic for several reasons previously outlined by Denning. Critical among them is the question of whether cyber deterrence is limited to cyber types of punishment, or are other instruments of power available? Questions of redlines, escalation, proportionality, and survivability are germane to this discussion and should be framed before considering this dimension of deterrence.

The United States could work toward a deterrence by punishment strategy in several ways. First, a framework of international and domestic law should be established in at least two areas. One area involves guidelines associating cyber punish-

ments with cyber violations. The other area involves integrating and relating strategic domain actions (space and cyber) with traditional domain actions (air, land, and sea).[9] Here Manzo suggests establishing equivalent classes that are agreed upon by the international community, may be used to interpret the significance of actions across domains, and may avoid unintended escalation. Typically, this occurs through tradition and custom, but conflict in space and cyber are still normalizing. For example, should the United States decide to leverage its new naval laser technology as a potential space weapon, it should establish a framework that clearly establishes redlines and employment criteria.[10] Second, the United States could promote a cyber arms race complete with a showcase of exploit tools and a significantly large industrial base able to craft new exploit tools over time. Note that the deterrent isn't any particular exploit tool, but rather the industrial base that builds them. While this may lead to a space and cyber arms race, the counter argument might be that this is an eventuality, and the United States might as well seize the initiative. The key to developing a viable build-and-discard cyber weapon capability includes significant reforms or new authorities in the federal acquisition regulations. Third, the United States could take the initiative to preplace malware on their adversaries' critical infrastructure as a means of holding cyber terrain at risk. While demonstrating evidence of such preplaced capabilities might sacrifice the asset, planting the seed of doubt in the trustworthiness of their systems may pay dividends for years. If the United States were to highlight this exposure to other potential adversaries, the impact might reverberate across state-sponsored actors. Care would need to be taken to distinguish malware intended to create cyber effects versus malware intended to facilitate intelligence collection.

Fourth, the United States could entangle government and military systems with global civilian systems to change the calculus of deterrence. This approach assumes that an attack on the US government would be sufficiently egregious to the civilian population and world economy, and thus garner political support for full-spectrum options. The Global Positioning System (GPS) shares this characteristic in so far as an attack on it to degrade military operations would also impact civilian populations across the globe and help justify kinetic countermeasures.

Deterrence across a Range of Actors

Investments into deterrence strategies must account for potential attacks across a range of adversary actors. Whereas a nation-state might be more receptive to deterrence by punishment, nonstate actors may have little to hold at risk and therefore deterrence by denial or resiliency might be more appropriate. Historically, the US military has put disproportionately more effort towards denial strategies, with some growing efforts toward resiliency, because it requires little external coordination. However, nation-states are not deterred by these internal efforts because within their strategic calculus, the potential payout has historically far exceeded the risk of attribution and US action. The key to deterrence by punishment is to position something the adversary values at risk. For nation-states, perhaps this aligns with Col John A. Warden's centers of gravity theory.[11] For nonstate actors, the impact of

offensive cyber operations remains unclear.[12] Current theory suggests focusing on key leadership individuals and their immediate objectives.[13]

Recommendations

Increase Global Space and Cyber Situational Awareness

> *I think all warfare today requires interdependencies, coalitions, and partners. But in cyber, I think there is a more profound requirement to have partnerships in ways that are different than other military warfighting domains.*
>
> —Lt Gen J. Kevin McLaughlin, USAF
> Deputy Commander, US Cyber Command

Among the many concerns regarding space and cyber deterrence, attribution and transparency must be addressed if meaningful deterrence is desired. Each factor should include at least two components. First, the adversary needs to know that they have been caught red-handed and thus subject to justice. Second, potential adversaries need to observe that bad actors are held accountable for their actions to deter further undesirable behavior. In an age of encryption and spoofing, holding the offenders accountable may seem like an insurmountable problem, but one merely has to remember that cyberspace is, by definition, a man-made environment and thus malleable and mutable.[14] Instead of defaulting to an environment that allows end-to-end encrypted traffic to pass obfuscated through systems owned by nation-states; instead require traffic to be inspectable based on the laws of the hosting government.[15] This is not to say that all traffic will be inspected, only that governments retain the right to inspect any good or service (in this case, information) that passes through their borders, even transient traffic. While some countries may not adopt this model; neither is the recipient of such traffic under any obligation to accept it, nor does the model impede public traffic. However, this model does provide collaborating governments with a means of detecting and tracing bad behavior, and more importantly, collecting evidence for closer inspection by the international community. Additionally, collaborating governments can assist each other to facilitate cyber attacks in a manner similar to allowing flight paths through friendly airspace, creating a more natural framework for coalition vice unilateral engagement. With evidence in hand, all instruments of national power across all domains become plausible.

Establish a National and International Framework

> *One thing the exercises have highlighted is the difficulty at times of determining the appropriate response due to a lack of rules of engagement in space. If we're going to act decisively in real time, we have to address these issues legally and operationally.*
>
> —Vice Adm Charles A. Richard, USN
> Deputy Commander, US Strategic Command

Closely related to the aforementioned investments into global space and cyber situational awareness, the need for a national and international framework for managing behavior in the global commons is paramount. Key among these needs is a requirement for governments to be accountable for space and cyber activities that are either sanctioned by or originate from their jurisdiction. While it may seem foolish on the surface to enact a law that is difficult to enforce, the true goal is to force a decision on state actors. Either the originator acknowledges that they are a space/cyber combatant and thus deals with the aftermath, or they claim the part of victim or bystander. In the latter cases, this opens an opportunity for the injured parties to shape the outcome by requiring additional laws, cyber security education, limitations on outbound traffic, or in extreme cases network isolation. The premise behind this strategy involves an expectation that states allowing technology to be used must first demonstrate the ability to govern it because of the potential for global impact.

Consider the idea of consolidating management of cyberspace and assigning the United States as the international steward for the benefit of humanity. While this may seem outlandish at first, reflect on the way that the United States already plays a similar role for space (GPS) and world currencies (US dollar as the world's reserve currency). The United States already influences much of the infrastructure (that is, domain name services) through research and development, and US companies (Google, Intel, Microsoft, and so forth) are directly involved in crafting cyberspace, so perhaps the US government might take a larger role in the employment of such technologies. Perhaps part of this role might involve the registry of devices and people allowed to use the Internet, thus striking a balance between privacy and security.

Strategically Develop Space/Cyber Military Operators and Citizen Militias

> *Cyber Airmen may attend professional developmental opportunities such as Air Force Institute of Technology, Computer Network Operations Development Program, or the Air Force Weapons School, all of which will positively impact the operationalization of the cyberspace domain within the Air Force and in turn, the future of the Cyber Mission forces.*
>
> —Maj Gen Chris P. Weggeman, USAF
> Commander, 24th Air Force and Air Forces Cyber

One of the key strengths of the United States and many western democracies is the freedom of innovation and industry. Investments into such programs as Cyber Patriot, National Collegiate Cyber Defense, and Advanced Cyber Education yield generations of citizens with cyber acumen (shown in figure).[16]

Showcasing the investment and resulting abilities becomes a strategic tool for deterrence since not only government agencies but also private corporations have a deep understanding of cyber security. However, deeper investments of computer science, engineering, and cyber operations into K-12 is needed to demonstrate a national commitment to our security and safety. This is much more than formal education, but rather a cultural change where cyber role models, children's television programming, and successful careers shape the attitudes of our youth. By building a national reserve of ethical talent, the United States not only enhances the cyber

resiliency within domestic companies and products, but may also draw upon this reserve in times of crisis. Whereas totalitarian regimes might limit the development of such talent in fear of regime overthrow, the United States might embrace ethical hacking in a manner similar to universal gun rights and ownership, thus giving the United States a strategic advantage. In a similar manner, the forecasted ubiquity of space travel through companies like Space X may create a similar deterrence effect where any attack on travelers may yield a conventional response, particularly if attribution and transparency are addressed.[17]

Courtesy Stacy Burns

Figure. Hannah Kirst (Texas A&M University), David Home (University of Colorado), Matthew Holt (Lock Haven University, Anh Bui (University of North Carolina at Charlotte) and Albert Bierley (University of California) are among the students benefitting from Advanced Cyber Education at the Air Force Institute of Technology in July 2017.

Update National Security Strategy and Joint and Air Force Space/Cyber Doctrine

> *I would argue that we should view cyber as one element of a broader deterrence campaign.*
>
> —Adm Mike Rogers, USN
> Commander, US Cyber Command

As previously mentioned in joint and Air Force doctrine, deterrence requires clearly communicated and credible threats along with a believable intent to exercise those threats. Current space doctrine emphasizes responsible behavior, partnerships that encourage restraint, collaboration toward quick attribution, and appropriate responses when deterrence fails.[18] However, current cyber doctrine specifies very little toward a deterrence strategy.[19] One might be tempted to adopt the same deterrence strategy across space and cyber, however, this may not work for several reasons. First, the cyber landscape changes more rapidly than space. Second, the United States has more deterrence options and actors in cyberspace. However, given the increasingly contested nature of both domains, the United States should be more explicit about taking action both within and across domains. Furthermore, enhancements

to the National Security Strategy might include the full spectrum of national instruments of power to realize this article's recommendations. A consistent strategy and doctrine will be key to safeguarding the nation.

Conclusion

> *It is unfortunate when men cannot, or will not, see danger at a distance; or seeing it, are restrained in the means which are necessary to avert, or keep it afar off. . . Not less difficult is it to make them believe, that offensive operations, often times, is the surest, if not the only (in some cases) means of defence.*
>
> —President George Washington
> 25 June 1799

In summary, the United States has reached an important crossroad as it contemplates the future of space and cyber deterrence. Historically strategic deterrence has worked, but applying such constructs to space and cyber domains remains challenging without better attribution, international laws, human capital investment, and updated national strategies and doctrine. Without these changes, space and cyber will remain niche and nuanced domains, susceptible to attack and exploitation, and in the worst case, our nation's Achilles' heel. As leaders entrusted to make sound investment decisions, we have the ability to shape not only space and cyber, but possibly our national destiny as well. ✪

Notes

1. Defense Science Board, "Task Force on Cyber Deterrence," Technical Report (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics), 1 February 2017, http://www.dtic.mil/docs/citations/AD1028516.

2. Andy Greenberg, "How an Entire Nation became Russia's Test Lab for Cyber War," *Wired*, 20 June 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

3. Lt Gen In-Bum Chun, ROKA (Ret.), "North Korea's Offset Strategy," in *Breakthrough on the Peninsula: Third Offset Strategies and the Future Defense of Korea*, ed. Dr. Patrick M. Cronin (Washington, DC: Center for New American Security, November 2016), 39–48, https://www.cnas.org/publications/reports/breakthrough-on-the-peninsula.

4. Martin C. Libicki, Edward Geist, Dorothy E. Denning, Stephen J. Cimbala, Frank J. Cilluffo, and others have identified challenges associated with cyber deterrence.

5. Edward Geist, "Deterrence: Stability in the Cyber Age," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015), 44–62, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-09_Issue-4/Geist.pdf.

6. Data compiled from the National Vulnerability Database, https://nvd.nist.gov; and Air Force Public Affairs Alumni Association, *Air Force Communication Waypoints 2017*, http://www.afpaaa.org/PDF/Waypoints0817.pdf, 20.

7. Sophia Chen, "Chinese Satellite Relays a Quantum Signal between Cities," *Wired*, 15 June 2017, https://www.wired.com/story/chinese-satellite-relays-a-quantum-signal-between-cities/.

8. Jeff Guion and Mark Reith, "Dynamic Cyber Mission Mapping," Institute of Industrial and Systems Engineers Annual Conference, 2017.

9. Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?" *Strategic Forum* 272, National Defense University Institute for National Strategic Studies, December 2011, http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf.

10. Michael Fabey and Kris Osborn, "Navy to Fire 150Kw Ship Laser Weapon," *Scout*, 23 January 2017, https://scout.com/military/warrior/Article/Navy-to-Fire-150Kw-Ship-Laser-Weapon-From-Destroyers-Carriers-101455353.

11. Maj Gary M. Jackson, USAF, "Warden's Five-Ring System Theory: Legitimate Wartime Military Targeting or An Increased Potential to Violate the Law and Norms of Expected Behavior?," Research Report (Maxwell AFB, AL: Air University Press, April 2000), www.dtic.mil/get-tr-doc/pdf?AD=AD A425331.

12. Jeff Seldin, "Cyber War Versus Islamic State 'Work in Progress,' " *Voice of America News*, 18 May 2016, https://www.voanews.com/a/cyber-war-versus-islamic-state-work-in-progress/3336773.html.

13. Statement of Dr. Craig Fields, chairman, Defense Science Board, and Dr. Jim Miller, former undersecretary of defense (policy) and member, Defense Science Board, in "Cyber Deterrence," unclassified testimony before the US Senate Armed Services Committee, 115th Congress (Washington, DC: 2 March 2017), https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller_03-02-17.pdf.

14. Mark Reith, Seeley Pentecost, Daniel Celebucki, and Robert Kaufman, "Operationalizing Cyberspace: Recommendations for Future Research," International Conference on Cyber Warfare and Security, March 2017, https://search.proquest.com/openview/0c3e05994e4a362d80ad6374fb1b10e9/1?pq-origsite=gscholar&cbl=396500.

15. This is accomplished by decrypting and reencrypting traffic at each segment of the traffic's journey using public key infrastructure technology. This would clearly create multiple privacy concerns; however, history reveals that societies are continually reshaping expectations of privacy against the need for security, and the concept of privacy has grown in proportion to technology, self-sufficiency, and wealth. Ergo, the concept of privacy is not an absolute right, but rather a privilege determined by the community.

16. The Air Force Institute of Technology hosts Advanced Cyber Education, https://www.afit.edu/ace/news.cfm.

17. Don Lincoln, "Elon Musk is Changing the Rules of Space Travel," *CNN*, 1 April 2017, http://www.cnn.com/2017/04/01/opinions/elon-musk-change-rules-of-space-travel-lincoln/index.html.

18. Joint Publication (JP) 3-14, *Space Operations*, 29 May 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

19. JP 3-12, *Cyberspace Operations*, 5 February 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Lt Col Mark Reith, USAF, PhD

Lieutenant Colonel Reith (PhD, University of Texas at San Antonio) previously served as deputy commander of the 26th Cyberspace Operations Group and commander of the 690th Network Support Squadron, leading enterprise cyber defense and Department of Defense Information Network forces respectively. He currently serves as director of the Center for Cyberspace Research and assistant professor of Computer Science at the Air Force Institute of Technology.