Summer 2018

# Cyber War and Deterrence: Applying a General Theoretical Framework

Isaac Nacita [*]
*Air Force Institute of Technology*

Mark Reith
*Air Force Institute of Technology*

# Cyber War and Deterrence

## Applying a General Theoretical Framework

Capt Isaac Nacita, USAF
Lt Col Mark Reith, USAF, PhD



### Introduction

> *Military history, when superficially studied, will furnish arguments in support of any theory or opinion.*
>
> —Paul Bronsart von Schellendorf

In September 1870, after just six weeks of what many thought would be a prolonged war, Prussian bystanders jeered Louis-Napoléon Bonaparte as he was carried to captivity in what is now Kassel, Germany. It was a fitting portrait of French national disgrace.[1] Their military structures before the war and lack of strategic planning were partly to blame. National archivist Dallas D. Irvine points out, "it (the French system) was almost completely effective in excluding the army's brain power from the staff and high command. To the resulting lack of intelligence at the top can be ascribed all the inexcusable defects of French military policy."[2] Nevertheless, influenced by the idea that France had lost due to its lack of morale that an offensive approach would have provided, the military regrouped and refocused itself, this time adopting "attaque á outrance." This doctrine was French military strategy entering World War I, and it was almost immediately proved spectacularly wrong. The French lost 300,000 soldiers in the first month of war. Yet "the legacy of the adoption of the offensive was even more terrible in another sense. The wanton slaughter it spawned produced a similar reaction in all those who lived through it—a grim determination never to allow such slaughter again."[3] Once again, they turned to the defensive, and in the years leading up to World War II constructed the Maginot line. The Germans simply bypassed its strong points and broke through a weaker French line in unexpected terrain. The Maginot line is now a metaphor for something that creates a false sense of security.

There is a saying that politicians and generals are always fighting the last war, which is emphasized when the weapons and characteristics of warfare are changing rapidly. However, if this is true, it is often not due to an inability to learn lessons from previous conflicts, but to "overlearn" or overcompensate for the failures and experiences of the past. In reality, this is not a learning problem but one of forming poor implications from historical events, which leads to poor applications of doctrine the next time around.

The DOD now acknowledges that warfare has extended into cyberspace, and it is my central thesis that the military often suffers from a lack of meaningful conversation concerning the problems it faces in that domain. The lack of discourse is due partly to poorly adopted metaphors and analogies pulled from other domains of warfare and historical examples, and in general to a lack of rigorous strategic framing of the problem and its potential solutions.

## The Problem

What problem doesn't the United States face in cyberspace? The online world reflects the totality of human societal issues. Is there a cyberwar occurring? Cyberspace is a "contested environment," but so is the global business market. Karl Von Clausewitz called war a clash of wills, a political act carried out by other means, yet also characterizes it with physical force that seems to require a physical domain.[4] Some, therefore, argue that acts of sabotage, espionage, and subversion occur, conducted through a different medium, but not warfare.[5] Martin C. Libicki suggests the possibility of "sub-rosa" warfare, implying the general population may be totally unaware of what is occuring.[6] Others downplay the terminology because what we have faced so far is overhyped and does not merit the title. In many cases the actual effects due to malicious cyberspace attacks are less than those that occur due to natural or accidental events. There is a somewhat humorous incident in which, a year after alleged Russian cyber attacks in Georgia, a 75-year-old woman accidentally cut a cable with a shovel and knocked out internet access in all of Armenia, outdoing Russia in terms of total effect.[7] All of this is also compounded by the tendency to treat all of America's social problems using warfare terminology. We are fighting a "war against poverty" and a "war on drugs." There is winning, and there is losing but rarely a clear winner or loser.

These things notwithstanding, the DOD has already recognized cyberspace as a war-fighting domain. But the nature of the problem is central to the question of deterring or prevailing in cyberspace. One source says, "stop debating on what to call the problem and get us some help!"[8] The point is understood, but if the problem is not, we should not expect to receive any meaningful help.

The Defense Science Board (DSB) presents some examples of cyber attack that may be used to frame the problem. It points to Iran's denial of service (DoS) attacks on Wall Street in 2012–13, North Korea's hack of Sony Pictures, Chinese intellectual property (IP) theft, and Russia's alleged involvement in the 2016 presidential elections. The document also refers to attacks by nonstate actors like Anonymous or New World Hackers, acknowledging that all of these represent only a small sampling. Fears

include the ability of these nations to hold US critical infrastructure at risk, to thwart American military response via the cyber domain, and to use a wide range of lower-intensity attacks that collectively take a toll on the foundations of national power.[9]

The DSB's recommendations for cyber deterrence read like a Cold War deterrence playbook and not without acknowledgement. Its first initiative, planning tailored deterrence campaigns to cope with a range of attacks, unmistakably resembles flexible response, the concept that moved US nuclear policy away from massive retaliation toward something more proportional. Its second initiative, creating a cyber-resilient "thin line" to key US strike systems, even uses the term "second strike" in a clear acknowledgement of its nuclear deterrence forbearers. Even "countervailing" appears in the document, a term used during the Carter administration years to convey a particular nuclear deterrence strategy.[10] The analogy is not limited to the DSB, presumably because the cold war itself is often invoked in discussions of the relationship between countries over their interactions in cyberspace.[11] A recently cited case described the suggestion to leak our cyber offensive capabilities, which takes the idea from nuclear deterrence, that is, a secret weapon cannot be a deterrence.[12] Even the question posed for this article seems to echo President Reagan's speeches on "prevailing" over the forces of communism and the Soviet Union.

In 2012, Defense Secretary Leon Panetta used the term "cyber Pearl Harbor" to convey the danger the US faced in the cyber domain;[13] others have similarly used "Cyber 9/11." In contrast, John Arquilla and David Rondfeldt suggested (more than a decade earlier) a "manifest destiny for the information age."[14] Others call cyberspace the new "wild, wild west" or harken the era of pirates and privateers, weak governments, and inexplicit or unenforced international norms.[15] All of these have something in common: the desire to explain something new in understandable terms by reminding us of the past. Cyberwar is complicated because it covers a range of attacks; DoS attacks and leaking of Democratic National Party documents represent two very different types of attacks and two very different strategies. The only thing they really have in common is that both were conducted using cyber domain tools and directed at the US.

Scholars have noted that metaphor is an essential part of how humans rationalize and understand the world, not just in language, but also thought processes.[16] Christopher R. Paparone argues that "management of meaning" is a primary task for leaders.[17] They are often the best way to frame the narrative, but with the obvious problem of oversimplification. A naïve translation of nuclear deterrence principles into cyberspace, therefore, obscures the real problems we face.[18] Metaphors "carry with them, often covertly and insidiously, natural 'solutions.' "[19] Computer viruses resemble biological viruses, so some have suggested a cyber version of the Center for Disease Control.[20] Online piracy, like real piracy, is a problem of establishing international norms and compelling nations to enforce them.[21] These are perhaps two of the better ideas, but they also show that the method of framing the problem affects the way the solution is formulated. Winston Churchill's iron curtain description painted a visceral image in Western minds that helped to shape the policy of containment under the Eisenhower administration. References to an "information curtain" or "tearing down this firewall" lack the same vitality.[22]

Paparone discusses categories of metaphor used by leaders: Newtonian, post-Newtonian, and Humanities and Arts.[23] Newtonian metaphors are based in the hard sciences, and tend to be deterministic in character. Military doctrine derives many of its concepts from Newtonian terminology, such as mass, friction, center of gravity, and power, which carry a quantitative quality. In contrast, post-Newtonian metaphors allude to the complexity and mutual interaction of a system, based in fields like biology, medicine, and quantum mechanics, in which probabilistic effects characterize outcomes rather than linear, deterministic ones. The terms are used extensively in the cyber domain; network, virus, infection, and worm all draw parallels to the "post-Newtonian" world. They are also used to explain things like terrorism and insurgency. Finally, the humanities and arts provide metaphors and analogies from historical, literary, and cultural references. In one of the better war metaphors, Clausewitz likened it to two wrestlers striving for dominance over one other.[24]

In summary, the cyberwar discussion is taking place within a language context that is as congested as the internet itself. This problem has some precedent. Lt Col Peter Faber, USAF, retired, argued that airpower theory and doctrine suffered inside a similar "prison house of language" during its development that mixed rationalist ideals, antirationalist thought, and army terminology.[25] In response, Lieutenant Colonel Faber suggested a framework originally conceived by Dr. Robert Pape and expanded by several works at the Air University.[26] This framework was intended to generalize the ideas of airpower, but without locking it into a particular linguistic context. Particularly, the goal of any strategy is to link ends with means. It is this framework that I propose can be utilized to help understand how to address the cyber-specific threats to national security that the US faces.

## A Strategic Framework

The framework takes the form of six key questions in anticipation of any strategy utilizing military forces:[27]

1. What outcome am I seeking?
2. What are my specific politico-military capabilities and those of the adversary?
3. What type of strategy should I pursue?
4. What targets or objectives are most important?
5. What mechanisms do I expect my operation to trigger?
6. How should I time my actions?

Beginning with the first question, the outcome sought is primarily political in nature. However, it does not have to be destruction-oriented. In this case, the aim is to stop aggressive actions in cyberspace. Yet this requires further clarification. The outcome should be considered with respect to some receiver.[28] Who should stop conducting aggressive actions in cyberspace, and which actions should stop? Is the political outcome that China reduce IP theft from American corporations? Or is it to reduce the vulnerability of US critical infrastructure? Changing the formulation of

this outcome may change the direction of the strategy. For instance, the outcome may be stated in terms of stopping a particular nation-state from taking hostile cyber-actions against our power grid. Alternatively, it may be stated in terms of minimizing the *effects* of a power system cyber attack on the functioning of society. In the latter case, perhaps the receiver is not the adversary but the private owners or managers of US critical infrastructure. We should avoid the temptation of grand, unified strategic deterrence aims to cover all possible cyber actors and activities; such a thing is akin to a "land" or a "sea" deterrence.[29]

Next, the comparison of politico-military capabilities. Policy, readiness, training, domestic culture, equipment, tactics, and attribution are all applicable in the cyber domain as in every domain. Perhaps the US holds a conventional warfighting advantage, but how ready are forces to defend networks or conduct offensive actions in cyberspace? What about cultural strength, the responsiveness of the general populace to an information campaign pressing a particular narrative, as in alleged election meddling? Sun-Tzu may have summarized the importance of this question simply: know yourself, and know your enemy.[30]

The third key question asks that a particular strategy be considered. Lieutenant Colonel Faber suggests several:

- punishment—pushing a society past its economic or psychological breaking point
- risk—same as punishment but with gradual escalation
- denial—neutralizing ability to wage war
- decapitation—destroying or isolating leadership, national communications, or other centers of power
- disabling—disrupting offensive abilities
- delaying—using threats or deterrence method to preserve status quo
- enabling—creating stability where it is weak

It now becomes clearer why language problems have often been crippling to cyber discussions. Nuclear deterrence analogies, which have been used but found wanting in most cases, do not usually fit because they were formulated for specific political outcomes and specific assessments of capability. It is of course true that cyber weapons aren't nuclear bombs, but bombs were not the goal of deterrence, they were the means that fit the assessment. A more important lesson is how, not what, strategy was applied given the options. The delaying or punishment strategies may have worked then; maybe a denial or an enabling strategy is more appropriate now. A possible example of a "cyber" decapitation strategy was the release of the Mandiant report, which simply used well-documented exposure of the PLA to isolate it in the international community.[31] This led to international agreements, with observed decreases in the number of cyber intrusions since.[32]

The fourth key question regards critical targets and their importance. Lieutenant Colonel Faber points out issues to consider:

1. Which aspects of the receiver's power should be targeted?[33]

- Sources – military, industrial, cultural
- Manifestations – government, ideological
- Linkages – human and material networks

2. What is the generic strategy?
   - Direct – "head on" assault, confrontation, or support
   - Indirect – reduce will to fight or alter decision making
3. What level of destruction do I want?

Clearly, the previously mentioned adversaries make the same considerations. The indirect strategy is often assumed in cyberspace, which sometimes is translated denial, degradation, disruption, destruction, or manipulation of information.[34] In a general sense, however, a target may be chosen for either strengthening or weakening, depending on the previous formulations.[35] Targeting theory forms a large part of airpower theory and is a key aspect of nuclear strategy. The US also often uses economic leverage to target sources of power. Cyber-targeting is a less developed concept but was recently considered in a thesis at Air University.[36] As with airpower, the targets are endless. However, the linkage between this step and the next is what Lieutenant Colonel Faber refers to as the "holy grail" of airpower, something that has yet to be completely achieved.

The fifth key question is to ask which mechanisms are expected to be activated by the previous targeting choice. What changes or outcome should be expected? Political division? Mass confusion, revolt, or surrender? Increased will to fight? A key reminder from early airpower advocates is that they were often wrong; bombing cities sometimes resulted in chaos or surrender and sometimes strengthened the people's will to resist. Cyber power effects are similarly difficult to predict. The 2007 DoS attacks in Estonia do not appear to have achieved any lasting effect. Stuxnet delayed but did not seem to ultimately alter the direction of Iranian nuclear programs. On the other hand, understanding the real effect of the information campaigns during the 2016 election remains elusive. First-order effects in cyberspace are easier to calculate, as they were in strategic bombing, or they may not be the primary purpose at all. It is the second, third, and fourth-order effects that have always been difficult, and these depend greatly on whether proper attention has been paid to question two.

Ultimately, deterrence is not a matter of thwarting technology, but of influencing decisions. These decisions are usually specific and limited. US nuclear policy perhaps influenced Soviet decisions to not launch nuclear weapons but did not prevent every undesirable Soviet military action, because there is no way to guarantee human behavior in every situation. However, one can use critical thinking and good judgment to seek solutions if the problem is framed well, the desired outcome is clearly defined, and the work to know ourselves and our adversaries well enough to make reasonable estimates of their responses has been done.

Finally, Lieutenant Colonel Faber considers timing. Should actions be single or multiple? Incremental, sequential, cumulative, or simultaneous? Once again, this is

tied to the desired mechanism. Will a single response be enough to deter a particular actor from a particular behavior? Or actions taken on a regular basis? Declaratory policy may work in some cases and may not in others.

It is my assertion that this framework provides a helpful, yet nonprescriptive manner in which to gauge the question of strategy for war and deterrence in cyberspace. It is not prescriptive because war is ultimately not a deterministic mathematical equation, and linking means and ends has always proved difficult. Nevertheless, it reminds us of a few important lessons, and helps free us from the traps of communicating under a constrained set of references.

## Some Final Recommendations

What then, should the US do to better prepare for deterrence and, if that fails, to prevail in cyberspace? There are at least three ideas that we should grasp from this exercise.

1. Critical thinking and judgment must replace lessons learned.

> *They said, that to go to the gate for entrance was, by all their countrymen, counted too far about; and that, therefore, their usual way was to make a short cut of it, and to climb over the wall, as they had done.*
>
> —John Bunyan, *Pilgrim's Progress*

The central idea of this article has been that a poor usage of language and a lack of framing the problem has complicated and crippled the discussion of cyberwar and deterrence strategy. Senior leaders will not and should not throw out all metaphorical language and historical references. Our language and our history are part of our country's strength. Therefore, communication of the right pictures and the right historical lessons for the purpose of formulating today's strategy remains the goal. This will happen to a greater degree when we commit ourselves to the hard task of critical thinking rather than taking the shortcut of a simplified lessons-learned approach. We must learn from those who considered nuclear warfare in the 1960s, or asymmetric warfare in the Middle East, but we should not try to take shortcuts in our solutions. We must consider problems on their own merit, while acknowledging the work of those before us, and reaping the benefit of strategic thinkers who helped provide a framework for thinking well today.

2. Courageous leadership will be required.

> *Never neglect the psychological, cultural, political, and human dimensions of warfare, which is inevitably tragic, inefficient, and uncertain. Be skeptical of systems analysis, computer models, game theories, or doctrines that suggest otherwise.*
>
> —Secretary of Defense Robert Gates, 2008

Decisions in war and peace are often based on insufficient intelligence, probabilities, and general principles. We can reduce the likelihood that we make fundamentally unsound links between our ends and our means by thinking clearly and critically and taking into account a broad set of perspectives. However, at the end of the

day, our leaders will have to be courageous enough to listen and courageous enough to act or not to act. We should expect nothing less. War is fundamentally uncertain, and courage to decide will always be required.

3. Humility is key.

> *A generally useful way of concluding a grim argument of this kind would be to affirm that we have the resources, intelligence, and courage to make the correct decisions. That is, of course, the case. And there is a good chance that we will do so. But perhaps, as a small aid toward making such decisions more likely, we should contemplate the possibility that they may not be made. They are hard, involve sacrifice, are affected by great uncertainties, concern matters in which much is altogether unknown and much else must be hedged by secrecy; and, above all, they entail a new image of ourselves in a world of persistent danger. It is by no means certain that we shall meet the test.*
>
> —Albert Wohlstetter, The Delicate Balance of Terror, 1958

Humility allows us to do several things. It allows us to consider the past and recognize that we are not unique in facing problems and challenges of humanity. It insists that we recognize and accept strategic miscalculations and change our course of action. It gives us the ability to work with others from different fields and different backgrounds to solve a common problem. It dictates that we defer to others who are more able, more knowledgeable, and more informed about particular areas that we will have to consider. It causes us to realize that complete answers and complete solutions are not part of the realm of warfare and deterrence. Finally, humility reminds us that it is not certain we will be successful and so shows us that we too must do the hard work that every past generation has faced in its own way. ✪

## Notes

1. Charles W. Sanders Jr., *No Other Law: The French Army and the Doctrine of the Offensive*, Research Report no. P-7331 (Santa Monica, CA: The RAND Corporation, 1987), https://www.rand.org/content/dam/rand/pubs/papers/2005/P7331.pdf.
2. Dallas D. Irvine, "The French and Prussian Staff Systems Before 1870," *The Journal of the American Military Foundation 2*, no. 4 (Winter 1938): 192–203.
3. Sanders, "No Other Law," 192–203.
4. Karl Von Clausewitz and Sun-Tzu, *The Book of War: Sun-Tzu's "The Art of War"* and Karl Von Clausewitz's *On War* (New York, NY: Random House, Inc., 2000).
5. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, doi: 10.1080/01402390.2011.608939.
6. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
7. Peter W. Singer and Noah Shachtman, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive," *Brookings Institute*, August 2011, https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/.
8. Jason Andress and Steve Winterfield, *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners*, 2nd ed. (Waltham, MA: Syngress, 2014).
9. Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2017), http://www.dtic.mil/docs/citations/AD1028516.
10. Sandia National Laboratories, *U.S. Strategic Nuclear Policy: A Video History, 1945–2004* (Albuquerque, NM: Sandia National Laboratories, 2012), https://archive.org/details/U.s.StrategicNuclearPolicy.

11. David Ignatius, "Cold War Feeling on Cyberspace," *RealClearPolitics*, 26 August 2010, https://www.realclearpolitics.com/articles/2010/08/26/cold_war_feeling_on_cybersecurity_106900.html.

12. Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York, NY: Oxford University Press).

13. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security," Department of Defense Press Operations, news transcript, 11 October 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

14. John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: toward an American Information Strategy* (Santa Monica, CA: RAND Corporation, 1999).

15. Singer and Friedman, *Cybersecurity and Cyberwar*.

16. Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7: (2 July 2012), http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270&sa=U&ei=E9hVU4_PBKrw8AGmhIDQC#p6.

17. Christopher R. Paparone, "On Metaphors We Are Led By," *Military Review* (November–December 2008), http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/2008-Archive/#novdec.

18. Singer and Shachtman, "The Wrong War."

19. Lawson, "Putting the 'War.' "

20. Singer and Friedman, *Cybersecurity and Cyberwar*; and Lawson, "Putting the 'War.' "

21. Singer and Friedman, *Cybersecurity and Cyberwar*.

22. Nathan Hodge, "Hillary on Net Freedom: Tear Down This Firewall," *Wired*, 21 January 2010, https://www.wired.com/2010/01/secstate-clinton-on-net-freedom-tear-down-this-virtual-wall/.

23. Paparone, "On Metaphors."

24. Clausewitz and Sun-Tzu, *The Book of War*.

25. Lt Col Peter R. Faber, *Competing Visions of Aerospace Power: A Language for the 21st Century*, research report (Newport, RI: Advanced Research Department, Naval War College, 21 February 1997), http://www.au.af.mil/au/awc/awcgate/theorists/faber-full.pdf.

26. A description of the development of this framework, as well as alternatives, is given in the following paper: Thomas P. Ehrhard, Making the Connection: An Air Strategy Analysis Framework, School of Advanced Airpower Studies (Maxwell AFB, AL: Air University Press, 1997), http://www.au.af.mil/au/aupress/bookinfo.asp?bid=438&type=papers.

27. Lawson, "Putting the 'War.' "

28. A note is important here: these strategies were formulated in the context of airpower. Nevertheless, the ends of airpower have always been considered strategic. Deterrence is an inherently strategic concept, and the general considerations should apply, not only with an offensive focus, but a defensive one as well.

29. The object of deterrence or offensive action is a person, not a technology or a domain, as described further in this article. Faber lists several: an international organization, a nation-state, a nongovernmental organization, a terrorist network, and so forth. However, our receiver does not have to be the adversary; it may well be an ally. An example of this is the Berlin Airlift, which sought to ensure West Berlin did not fall to Soviet economic pressures. In this case, the adversary was the Soviet Union, but the receiver was the people of Berlin. Presumably, there is some adversary, but our outcome need not be formulated in their terms alone.

30. Clausewitz and Sun-Tzu, *The Book of War*.

31. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly 77,* (Spring 2015), http://ndupress.ndu.edu/JFQ/JointForceQuarterly77/tabid/12113/Article/581864/rethinking-the-cyber-domain-and-deterrence.aspx.

32. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; and FireEye iSight Intelligence (2016). *Redline Drawn: China Recalculates Its Use of Cyber Espionage* (Milpitas, CA: FireEye iSight Intelligence, 2016), https://www.fireeye.com/content/dam/fireeye-www./current-threats/pdfs/rpt-china-espionage.pdf.

33. Once again, this is the receiver, which is not necessarily equivalent to the adversary.

34. Curtis E. Lemay Center for Doctrine Development and Education, 30 November 2011, *Annex 3-12—Cyberspace Operations: Introduction to Cyberspace Operations*, http://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-12-Cyberspace-Ops/.

35. For example, if the receiver is the adversary, its military power may be targeted directly through kinetic force or by cyber means. In the case of critical infrastructure, one may seek to change for the better the network security practices of the companies that manage those facilities by incentivizing or otherwise motivating better defensive practices.

36. Steven Anderson, "Airpower Lessons for an Air Force Cyber-Power Targeting Theory," *Drew Paper* No. 23 (Maxwell AFB, AL: Air University Press, 2016), http://www.au.af.mil/au/aupress/digital/pdf/paper/dp_0023_anderson_airpower_lessons.pdf.


**Capt Isaac Nacita, USAF**

Captain Nacita (BS, University of California at Los Angeles) is a master's student at the Air Force Institute of Technology, where he is studying space systems. Previously, he was an analyst at the 746th Test Squadron at Holloman AFB, New Mexico, where he led an element responsible for testing navigation and guidance systems.

**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.