Battlefield Geometry in our Digital Age

From Flash to Bang in 22 Milliseconds

By Robert Allardice and George Topic

This year has been tough for cybersecurity programs. Every month in the first six months of 2017, the world experienced a major cyber event. Open-source attacks included attacks on critical infrastructure, banks, intelligence services, and significant commercial and government entities. Indeed, reflecting on the scope and depth of most publically acknowledged compromises, uncovers the reality of the tremendous and growing risks the country faces nearly two decades into the 21st century. Everything seems to have changed. Virtually every organization within the Department of Defense (DOD) has, sometimes reluctantly, come to embrace digital age technology, to the point that they are completely dependent on it. The result is a shocking degree of paralysis when our access to the services we now rely upon is disrupted.

The paradox DOD faces is that the asymmetric advantage delivered by application of digital age tools can easily become an asymmetric disadvantage. That is, the very advantage gained through the speed, connectivity, and non-linear impacts delivered by leveraging the benefits of cyberspace, may be disrupted or denied with counter levers delivered by adversaries through the same medium. Is the United States, and more specifically DOD, prepared to deal with this?

This article describes a simple model that not only will give military commanders the highest probability of mission assurance but is applicable for the 99 percent who have become dependent upon cyberspace and digital age tools. Unfortunately, the 800-pound gorilla in almost every organization is: "What do we do if the systems delivering the knowledge and data are corrupted, exfiltrated, or denied?" Cyberattacks occur with little or no warning—from "flash to bang" in 22 milliseconds, or sooner—and victims often are unaware of an intrusion until significant quantities of data are impacted. A set of precepts is also proposed that can assist leaders in developing, arranging, and exercising the people, processes, and tools that will optimize capabilities and give commanders the highest probability of mission assurance on the digital battlefield. As a final point, a series of general recommendations is provided for consideration by leaders, managers, and policy makers at all levels to help manage the manifest challenges before us.

Lieutenant General (ret.) Robert Allardice previously served as Vice Commander, U.S. Air Mobility Command. He is a senior civilian mentor for Joint Force Development (J7) and a Senior Fellow at National Defense University. Mr. George Topic is Vice Director, Center for Joint and Strategic Logistics at Ft. McNair.

It is important for leaders at all levels to truly understand the nature of what is needed and to not mistake activity for progress or, even worse, victory. One of the most pernicious and dangerous responses to questions about cyber defense issues is, "We have already got that covered."

The New Battlefield

The digital age has changed battlefield geometry. In fact, the changes to warfare during the past several decades have been so profound that many central tenets of military theory enduring for generations or even millennia no longer apply—in some cases they are actually dangerous. Perhaps the best illustration of this point is the recognition that the battlefield is no longer physically bound or adequately described within the narrow frame of traditional kinetic effects. The speed, connectivity, and non-linear nature of the environment in which warfighters must operate, fundamentally changes how one must think about objectives and the threats we face. The geometry that has been used throughout history may no longer apply. Not only are physical boundaries less relevant, but the many dimensions or domains of warfare are also more closely integrated than ever before. Failure in any facet may compromise the entire mission and put the force and the nation at risk.

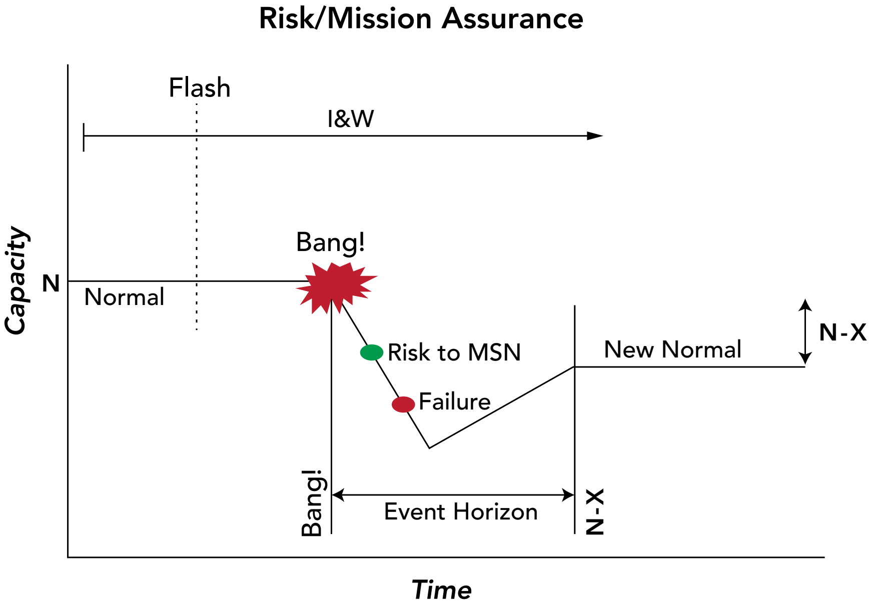
The Cyber Mission Assurance Model depicted in Figure 1, is derived from a RAND Corporation study and is intended to help leaders think through the challenges they face.[1] It can also provide the intellectual framework to develop the ability to survive and operate in a cyber challenging environment. The following paragraphs give an in-depth presentation of the model.

Ability to Survive and Operate: A linear Model to Assess the Current Challenge

First, a description of the model itself. Note, the vertical axis represents capacity and the horizontal axis represents time. Capacity, or organizational output ("N"), represents a notional, normal, sustainable level. At some point following along the timeline, an event occurs, labeled "bang." This is often that painfully obvious moment of an attack, intrusion, or other negative effect, occurring and impacting an organization. Generally an event is preceded by a "flash," an indication that the event is imminent or underway. Once an event occurs, the model shows a decrease in capacity at a given slope. At some point capacity is diminished to a level that puts the mission at risk. If capacity continues to decrease, at some discernable point, mission failure is imminent. Of course, as the organization reacts to the event, mitigation measures often begin to restore capacity at a given rate to a new

The geometry that has been used throughout history may no longer apply. Not only are physical boundaries less relevant, but the many dimensions or domains of warfare are also more closely integrated than ever before. Failure in any facet may compromise the entire mission and put the force and the nation at risk.

FIGURE 1: Cyber Mission Assurance Model.



"normal" labeled "N–X."[2] Each event has a life cycle labeled here as the event horizon. Finally, preceding an event, and throughout the event horizon, indications and warnings (I&W) provide data to inform decisionmakers at a level of detail that they are able to visualize the battlespace.[3]

Many immediately grasp the application of the model in a general sense, and more specifically when applied to the multi-domain problems presented by the modern battlefield. In basic terms, one can see how this simplistic model illustrates what most encounter as missions are accomplished. Consider capacity; most organizations have a set of capabilities that produce some type of capacity. This could be a product or a level of service. In the case of military organizations, at the highest level, the product is ultimately combat capacity. Organizations within DOD and other government agencies, usually spend a great deal of time measuring their ability to generate capacity. During peacetime, the military maintains a fairly consistent capacity to deter war and to prosecute a steady state-level of small conflicts. During times of total war or significant increase in demand, the nation mobilizes to a higher level.

Organizations performing at normal capacity often have I&W available to them essentially to identify threats to their ability to accomplish their mission with sufficient time to begin mitigating measures. Threats to the mission are often assessed from a risk perspective— i.e. how much risk does a particular threat present to the mission? For example, historical data shows significant weather events during the fall season so airports on the East Coast will look for indications of tropical storms. At some point, a hurricane may actually develop and the system will produce warnings of the direction, strength, speed, and potential impact of the storm. If a hurricane poses a significant risk to operations, airport leadership will order evacuations or take other mitigating actions. Looking at the model, notification of an imminent hurricane would be a flash.

When bang actually occurs with an impact that degrades mission performance (reduced capacity), the effect may be sudden or gradual reflected by the slope of the line. A catastrophic event can cause a total collapse which would be a near vertical slope, while a shallow slope would indicate a gradual decrease in capacity. As event impact increases or endures, at some point the mission of the organization is at risk. If the event continues unmitigated, the organization will eventually become crippled past the point of meeting mission needs or the production demands. This point is called mission failure. In most cases, some form of recovery from the event mitigates the negative impact causing a positive rebound to the curve. Again, slope matters. A rapid recovery is indicated by a steeper climb and decreases the event horizon time.

Broadly speaking, the role of the decisionmaker throughout the event consists of; setting the conditions to understand the I&W prior to the event occurring, ensuring the right processes and plans are in place to implement mitigation measures once flash has occurred, ordering mitigation measures when appropriate, and once bang has occurred, initiating reconstitution measures. Note using the hurricane example, many military organizations, particularly those that have suffered through a catastrophic hurricane, put considerable energy into planning and exercising in anticipation of future hurricane events. They have learned the value of actions left of flash, and sadly in some cases, the consequences of inattention left of flash.

Leaders should use variations of this model to think through and explain almost any event that impacts mission, not simply cyberattacks. Leaders want to perform at a designated capacity and to recognize events and risks with sufficient time to mitigate negative impacts. Generally, an organization's objective is mission assurance. All of the services, agencies, and commands within DOD have invested, and will continue to invest, in multiple systems to ensure they are able to accomplish their mission.

The interdependence of the cyber domain with all other domains presents significant risk profiles, and suggests the need to think through this concept of mission assurance from a different perspective than the current and historical "three-dimensional warfare."

Unfortunately, application of this model through a multi-domain or cyber lens exposes complexities and risks that should concern all leaders. The interdependence of the cyber domain with all other domains presents significant risk profiles, and suggests the need to think through this concept of mission assurance from a different perspective than the current and historical "three-dimensional warfare." Threat vectors are not just from air, land, sea, or space, but can come from any direction through the internet; in the cyber domain distance is generally not a factor or limitation. Nefarious actors acting either under the sanction of a nation-state or, as stand-alone agents, can introduce risk to systems with devastating consequences. Another particularly vexing aspect of cyberattacks is trying to determine if one is at war at all. At what point is a cyberattack considered an act of war?

Now think through the model with the lens of a mission under threat of a cyberattack. Operating at normal capacity, leaders should understand specifically how dependent their mission is on cyber systems, just as they understand mission dependency on aircraft, ships, infantry, etc. The model demands a level of knowledge about systems in order to make informed decisions based on specific I&W. Success after bang rests largely on planning and exercising in a realistic way. Experience in the past has indicated a lack of realistic planning and a nearly wholesale propensity to ignore realistic exercises. In fact, most commonly in exercises, cyber events are either treated as "stand-alone" (non-dependent) or a "white card" issue explained away without demonstrating how the unit will actually accomplish the mission.

The temporal impact of events complicates everything. In this battlespace, events move from flash to bang at extreme velocity and can deliver profound and even lethal effects before the victim is even aware of the threat. We literally go from flash to bang instantaneously and may be on a significant slope of reduced capacity moving towards mission failure unknowingly.

Moreover, the impact from these events can last for years, undoing projects, programs, and relationships that took far more years to develop. In the well-documented and widely known STUXNET attack on Iranian centrifuges, while it is hard to accurately assess the actual impact, it is clear that it was significant. Beyond the physical destruction of a major portion of Iran's centrifuge inventory, a major clean-up and security review of their programs was also necessary for them to continue the programs with confidence that their equipment was not compromised. The recent cyberattack in the Ukraine involving Petya malware, not only significantly affected government and public service activities, but spread to many other nations, commercial firms, and other entities across Europe, and around the world. While this could have been a simple criminal ransomware attack, there is speculation that it could also have been politically motivated or an act of hostility by an adversarial nation. It is the uncertainty that such attacks foster that causes the most damage; in some cases, prevention or remediation causes processes to be slowed significantly, adversely affecting major decisions and operations.

Success in the digital age fight demands considering the implications within the context of this model and taking large steps left of flash to understand and mitigate potential impacts of cyber threats. Additionally, the integration of cyber system experts and operational system experts must be sufficient to rapidly comprehend when bang occurs, and the slope of the line. Moreover they must have appropriate resources and authorities to take immediate mitigating steps.

This model can be applied at strategic, operational, or tactical levels. While the implications are different for each, the application is appropriate at each level. Though this article focusses on DOD, when applying it at a strategic level, it is relevant for the entire national security enterprise. Let the reader also note, that in the deeply intertwined world of international and multinational relationships, systems, and processes, even trying to develop national solutions may not be adequate. As pointed out above with the Ukrainian Petya malware attack, cyber operations are difficult to contain within a geographic space. Electrons do not recognize international borders. Consequently, cooperation among nations plays a part in both prevention and remediation. Similarly, attacks and intrusions in the commercial sector can find their way into DOD systems.

Precepts of Digital Mission Assurance

So far, this article paints a bleak picture. Rational and reasonable reliance on digital age tools and processes has produced quantum improvements in the United States' military capabilities, and absolutely extends our asymmetrical advantages.

However, it also presents asymmetrical vulnerabilities when viewed from the context of the cyber threat. One may find it easier to ignore the problem than to invest what is necessary to deal effectively with this Rubik's Cube. Unfortunately, while there has been a great deal of discussion about the impact of cyber events, at lower organizational levels and broadly throughout DOD, there seems to be some degree of paralysis in determining what an individual commander or individual organization should be doing today to achieve a high-degree of mission assurance.

While the challenges in the cyber domain can seem overwhelming and cause uncertainty in leaders about what to do or even how to think about the problem, there are things every organization can, and should, be doing. To be clear, cyber defense in and of itself is not sufficient; it is truly the clearest expression of a 21st century Maginot Line imaginable. In fact, it is the assertion, and a central theme of this article, that one cannot defend against the threat completely, that one must structure a methodology to accomplish the mission within the realities of the new battlefield geometry. If it is not obvious yet, let it be clearly stated: an organization cannot wait for flash or bang. The focus must be on the need for actions left of flash.

A set of precepts has been developed for organizations, commanders, and leaders at all levels that will hopefully assist in framing how to prepare for, and deal with, the challenges of offering capacity and performing missions. The five precepts—hygiene, redundancy, alternative practices, passive defense, and active defense—emerged from observations and experiences working with organizations (particularly in the joint world of the U.S. military) that, are struggling to discover pathways to accomplishing their missions in light of the current and anticipated threat streams. There is nothing magic or ironclad about them either in phraseology or content. The precepts are not a list of independent, progressive, actions; rather, they are intended as a framework to apply simultaneously at various degrees depending on the current environment and understanding of the problem. Each of the precepts are described on an individual level and then finally described holistically in conjunction with the model in order to offer recommendations for the road ahead.

> *The five precepts—hygiene, redundancy, alternative practices, passive defense, and active defense—emerged from observations and experiences working with organizations (particularly in the joint world of the U.S. military) that, are struggling to discover pathways to accomplishing their missions in light of the current and anticipated threat streams.*

Hygiene

Follow the basic cybersecurity principles and guidance. While this precept is obvious, it continues to be one of the most challenging for most organizations. To ensure mission success, every level within every organization must comply with basic blocking and tackling efforts such as virus scanners, the use of credentials, and password discipline. These are the typical things cybersecurity experts indicate are critical to insure a minimum level of mission assurance. In reference to the model, hygiene consists of the individual and collective actions that prevent an easy bang for/from the enemy. Interestingly, there seems to be a persistent, misguided belief that imposing a set of rules by itself will accomplish cybersecurity. This simply is not true and is a particularly dangerous fallacy. In an organization of 100 people, it only takes one person to have a minor lapse in judgment or attention to compromise the whole system. In the cyberattack known as Buckshot Yankee, a flash drive inserted into a single laptop computer introduced a virus that took at least 14 months to clean out, and estimates of the damage range as high as $5.1 billion. Despite significant efforts to mandate rules, experts indicate a substantial number of organizations continue to be compromised by 10–20 percent of their employees who do not comply. Relying solely on hygiene is insufficient.

Redundancy

Aggressively and continuously pursue multiple pathways to accomplish the mission if a specific system is compromised. The concept of having redundant systems seems straightforward—if a system is compromised or attacked we need to have the ability to jump to another system that will accomplish the same objectives. This can be very expensive, but it is effective. The common mistake many organizations make is to assume they must have redundancy within their own organization; redundancy can be seen from a much more holistic perspective. For example, DOD may find it must rely on the commercial sector for redundant systems to accomplish some objectives if its systems come under attack. The key is to know which systems can be accessible that present redundant capabilities and the impact of moving to those systems. Experience has shown that organizations often rely on a system they see as redundant, and yet, they have not exercised or practiced it. When they eventually do exercise this perceived redundant system, they realize there are significant unintended consequences, or it does not provide the required capability.

Alternative Practices

Develop a non-cyber dependent backup process. The most common practice heard about when participating in exercises outside of the actual cyber force, is reliance on alternative practices. For example, when asked what happens if the system was attacked someone will say "we go to alternative, manual, practices." One hundred percent of the time when asked if an organization ever completely exercises the alternative practice to accomplish their mission, the answer has been "no." For some that have actually tried a degree of alternative practice, they have found many unintended consequences for other organizations within the enterprise. The best way to achieve success using alternative practices is to exercise them completely and thoroughly on a regular basis. The combination of redundancy and alternative practices should provide the basis for a "thin line" that can be operated and defended to provide some degree

One hundred percent of the time when asked if an organization ever completely exercises the alternative practice to accomplish their mission, the answer has been "no."

of mission assurance even under the most severe level of attack.

Passive Defense and Active Defense

Try to know as much as you can about the enemy and take specific, measured, and thoroughly coordinated steps with respect to the enemy. These two precepts are combined because of their common foundation. For both active and passive defense, there is a level of understanding and knowledge of the enemy to develop. Digital age battlefield geometry transcends traditional lines of communication, placing a new demand signal for this in-depth comprehension of the enemy beyond traditional boundaries. Defense is largely dependent on understanding the true environment, knowing the enemy and its intent, capabilities, and vulnerabilities. Behind every attack or threat there is ultimately a human. That human has a capability, a purpose, and an intent. That human may be acting as an individual actor, a terrorist's activity, or as part of a sanctioned government. Defense is not about building a modern Maginot Line, nor is this about handing the defense requirement to U.S. Cyber Command. These precepts are based on the fundamental obligation of every organization to take full ownership of the mission's success, a subset of which is to own the defense problem. Then, in conjunction with the experts, construct a strategy to raise the confidence to deliver mission assurance.

Passive Defense

Passive defense is to develop the understanding of the new battlefield geometry, the environment within which your organization must perform, the specific threats to the mission and, in conjunction with mission partners and cyber experts, construct the actions left of "flash" required to *block* the success of the enemy.

Active Defense.

Active defense is to develop the understanding of the new battlefield geometry, the environment within which your organization must perform, the specific threats to the mission and, in conjunction with mission partners and cyber experts, construct the actions left of "flash" required to *neutralize* enemy capability before it can be brought to bear. In most cases, for military application this includes inputs to the joint targeting process. This can be a critical point. Historically, the logistics community would not consider that they had reason to have input to joint targeting. However, within the context of the digital age battlefield, to assure mission success, the joint logistics enterprise should identify multiple threats to dependent systems which require active defense actions left of "flash." This will require a nontraditional analysis of the enemy and assessment based on comprehension of the battlespace.

It is often reported that organizations such as U.S. Transportation Command (USTRANSCOM), have as many as 200,000 intrusion attempts on any given day. The vast majority of those attempts are things that normal hygiene can mitigate. Those normal hygiene actions must continue. Simultaneously, efforts to defend against threat vectors using passive and active measures within the definitions offered above can substantially raise mission assurance confidence. Finally, knowing that defensive measures can fall short, aggressive efforts to expand access to redundant capability while developing and exercising realistic alternative practices should be a high-priority. It is incumbent on every functional and mission commander to understand the new battlefield geometry and the mission assurance mitigation measures that can address the thrust of the mission measures that lead to success.

Recommendations

Actions Left of Flash

The focus must be on the actions left of flash. While there are actions that are more applicable at some levels, or in some kinds of organizations than others, there are also actions that are universal. For example, undertaking a concerted effort to seriously exercise, think through, and rehearse a left of the flash event, can be done at any level. Experience shows that as more organizations (and leaders) exercise, think through, and rehearse left of the flash, comprehension rises, along with a recognition that success does not emerge in a vacuum. There are authorities senior government officials must grant, well left of flash, to put the right processes in place to execute the steps necessary to mitigate risk once I&W exceed the threshold of tolerance.

Enterprise Perspective

There are a number of other actions that leaders at all levels can take to reduce risk and improve resilience. The basic blocking and tackling that military organizations do routinely needs to be considered in the context of cyber threats to mission assurance. Understanding and carefully assessing not only internal processes, but how other organizations are affected by yours, is also universally important. As mentioned earlier, the impact of shifting to an alternative system may have a significant impact on others. Decisions made at a tactical level might in fact render moot the actions of a major organization or compromise a major mission set.

Last Known Good

Being able to reliably identify when the "last known good," or clean data set was available, is a key part of the mitigation and remediation of effects. Once again, this is a skill that is not easily or often practiced. Clearly the timeframes required are dependent on the missions being performed. Closely related to this is the delicate skill of looking for and assessing I&W. In some cases, oversensitivity, and attendant overcompensation, might be as damaging as the consequences of an attack.

National Security Strategy for the Digital Age

The language used in this article is specific to DOD, however, the understanding of the battlefield geometry makes it clear to us that any fight in the digital age transcends the ability of DOD to fully defend the nation. This new geometry requires a national security strategy that fully comprehends the thought, authorities, and cooperation within the government, through the interagency process, that can establish the thresholds and actions required to be prepared. Once enemy intentions become imminent, it will be too late. Flash to bang happens nearly instantaneously. Additionally, modern geopolitical circumstances require thinking and action well beyond the whole-of-government and even whole-of-nation, to include partners and allies in developing a comprehensive and aggressive digital age security strategy.

Comprehensive Approach

These issues apply across multiple, or even most, government agencies and deeply into the commercial sector where the ability to direct and control actions is limited. DOD must double down on efforts to include the commercial sector as equal partners in the application of the precepts described in this paper. This thinking becomes even more important when we consider that many aspects of the defense mission are wholly reliant on the performance of the commercial sector. The Commander, USTRANSCOM testified that 90 percent of his "traffic flows on unclassified networks to and from commercial providers."[4] Additionally, a great deal of the logistics supply chain relies heavily on the commercial sector, both domestically and internationally.

Manhattan Project

Finally, we recommend the admittedly unlikely, even glib possibility of using a "Manhattan Project" approach to making the kind of progress everyone knows is needed to optimize security in the volatile and uncertain world around and before us. It is our contention that we are not preparing adequately for the wars we are most likely to fight in the years ahead—we are not only risking our competitive advantage with near-peer competitors, but making it possible even for much less capable states and other entities to harm us. The nature of such an effort is well beyond the scope of this piece, but it seems clear that such an effort would be a worthwhile investment.

Conclusion

While trying to develop cybersecurity or mission assurance solutions and recommendations, we must acknowledge that there are no absolute or permanent solutions. There is no endstate, victory or "mission accomplished." In the same vein, any recommendations are at best guidelines and suggestions that individual leaders need to tailor to their mission, organizational needs, and resources. Inevitably, there are trade-offs and the task at hand is to optimize your outcome with the capabilities you have available. In an environment where it is difficult or virtually impossible to anticipate some threats, it is likewise a challenge to decide how to prioritize your efforts. In a large and resource-constrained bureaucracy such as DOD, it is tough to make a case for investing to protect against threats you cannot see or describe—only postulate vaguely about dire impacts. Similarly, trying to discern how much effort is needed is also vexing—and an area where continual reassessment is crucial.

It is important for leaders at all levels to make sure we truly understand the nature of what we need to do and to not mistake levels of activity for progress or even worse, victory. We have entered an age where eternal vigilance is required and we are never going to be able to claim victory. On the other hand, it will be quite obvious if we are defeated, and we might not even know that we have been attacked. One of the keys to minimizing our risk is to ensure that we are all aware of the panoply of efforts, initiatives, projects, programs, contracts, proposals, organizations, etc. that are all working on some part of building cyber defense capabilities. As noted above (and worth repeating), "we have already got that covered," is one of the most pernicious and dangerous responses to questions about cyber defense issues. It is our experience that the opposite is often true, so we encourage leaders at all levels to ask more questions and examine any such claims from a holistic or enterprise perspective.

On the battlefield of the digital age, knowledge is king! Protecting knowledge is an objective as old as warfare itself. When we think of actions left of the flash, we recognize the imperative of maintaining a pure/reliable knowledge base. Therefore, it is strongly recommended that leaders pursue a high degree of confidence that on any given day they have a pure knowledge base backed up, secured, and available to the decisionmakers that need it. This is often referred to as the last known good; unfortunately for many organizations it is actually the "last good hope." That is unacceptable. PRISM

Notes

[1] Don Snyder, George Hart, Kristin Lynch, John Drew, "Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems: Guidance for Where to Focus Mitigation Efforts," (Santa Monica, CA: RAND Corporation, 2015), available at <https://www.rand.org/pubs/research_reports/RR620.html>.

[2] Obviously, this could be "N+X," but not a normal result within desirable event horizons.

[3] That is the "hope" of I&W! Decisionmakers often do, and should, challenge the I&W process to ask, "Does our current I&W provide sufficient insight to accurately visualize the battle space?"

[4] *National Defense Authorization Act for Fiscal Year 2017 and Oversight of Previously Authorized Programs:*

Hearing on the U.S. Transportation Command Fiscal Year 2017 Readiness Posture, Before the House Committee on Armed Services Subcommittee on Readiness, 114th Cong., 109 (2016) Statement of General Darren W. McDew, USAF, Commander, United States Transportation Command.