Mad Scientist

The 2050 Cyber Army Technical Report

TRADOC G2

7 November 2016

This Page Intentionally Left Blank

Executive Summary

The Mad Scientist 2050 Cyber Army project explored the visualization of the Army's Cyber Force out to 2050 and its ability to address three major objectives of the Army's Cyberspace Strategy for Unified Land Operations 2025:

> What does the cyber environment look like in 2040-2050 (how will cyber influence the environment and the population? What will connecting look like / what will they connect to? What are the drivers influencing this or not)?
>
> How do we build an Army Cyber Force that can dominate the cyber domain in the context of the multi-domain battle concept to gain a position of relative advantage?
>
> How can we build shared goals and expectations as well as develop an understanding of roles and responsibilities in order to build and maintain partnerships with U.S., and international academia, industry, defense departments/ministries and other agencies to enhance cyberspace operations? What new ideas should we be considering?

Co-sponsored by the TRADOC G-2 and the Army Cyber Institute at the United States Military Academy, the 2050 Cyber Army project leveraged submitted papers, an on-line technology survey, and a 13-14 September Mad Scientist Conference that generated the insights synthesized in this report.

Cyber Challenges

As the newest warfighting domain and the first declared domain to be totally man-made, cyberspace poses multiple **domain dilemmas** for those who would characterize its role in military operations. The cyber domain poses unique physics of time and space, altering our normal perceptions of distance, proximity, and sovereignty while shifting significant portions of the command decision process towards human-machine solution approaches.

Planning predicaments range from the quandary of cyberspace visualization to having to treat cyber "terrain" metaphorically, accounting for the fact that only 4% (the Surface Web) is readily accessible. Intelligence activity is too often forensic and "post-factual" vice "pre-factual," and our approach to cyber planning authorities is highly asymmetric, both between defensive and offensive operations, and with respect to our adversaries.

The ever-accelerating rate of change in the cyber domain makes **cyber-casting** daunting indeed. The Department of Defense no longer has a dominant technology development role in shaping the architecture of cyber space. In an environment where battle results are indirect and difficult to observe and quantify, predicting cyber outcomes is problematic even in the near term.

The ubiquity and pervasiveness of the cyber domain presents a **categorization conundrum** wherein the broad relevance of cyber action in the physical, cognitive and moral dimensions of conflict present endless opportunities for categorization confusion.

Collectively, the cyber challenges generate an “alternative domain” experience that alters our normal expectations with respect to every component of the DOTMLPF-P model.

Strategic Context

Our **interests in cyberspace** are generally congruent to national interests, but with influences (and impacts) that are more global, reflecting the interconnectivity of cyber infrastructure. Paradoxically, our commitment to ready communication and agile data flows simultaneously affords our adversaries opportunity to undermine our interests while advancing their own.

Digitization and cyber technologies are general-purpose technologies that underpin a growing share of economic activity far beyond the information technology sector. The cyber domain and the digital economy at work within that domain will have increasingly strong **economic linkages** to the foundations of U.S. power. The economic impacts of the cyber domain, moreover, promise to be disruptive to a stable social fabric with a high potential to accelerate growing gaps in income and mobility.

The role of **deterrence** in the cyber domain is already a pressing strategic consideration. The problems of ambiguity and attribution in that domain are well known, and there are effectively no rules to constrain cyber conflict. The role of deterrence is not yet conclusively demonstrated in the cyber domain, although the U.S. has announced a two-pronged deterrence policy that will pursue both “deterrence by denial” and “deterrence by cost imposition.”

Army approaches to future cyber conflict will have to account for a broad, multi-echeloned array of **cyber strategies**. Higher level strategies include The White House International Strategy for Cyberspace and the DoD Cyber Strategy; within the Army the strategic context is addressed by the Army Cyberspace Strategy for Unified Land Operations in 2025, and the Army Cyber Center of Excellence Strategy.

To practice effective mission command, sustain its forces, provide critical intelligence, and communicate over the horizon, a nation must – of necessity – be a **cyber power**. The "barriers to entry" for cyber power status, however, are relatively low. Moreover, cyber power demonstrates a destabilizing capability / vulnerability paradox: the greater the reliance on advanced cyber capabilities, the greater vulnerability to disruption, diversion, and destruction.

DOTMLPF-P Insights

Because cyber theory is relatively immature, cyber **doctrine** has relatively weak and disputed theoretical underpinnings for categorization, principles, and similar tools of doctrine. Fundamental doctrinal ideas such as "levels of war" and "maneuver" struggle to migrate to the cyber domain; while traditional doctrinal imperatives to generate combined arms synergy and to seize, retain, and exploit the initiative maintain their primacy.

Organization solutions for the 2050 Cyber Army have begun with the stand up of the Cyber Mission Force, but the Army's future organizational approaches must account for technology trends that are simultaneously both centralizing and decentralizing. Organizational solutions in the cyber domain will include extensive use of interdisciplinary teaming and partnering. A fundamental organizational debate looms as proposals surface for a Cyber Service.

Cyber warriors are "knowledge workers" and as such will need more than "**training**;" they need a strong education in cyber fundamentals in order to deal with the dynamic complexities of the cyber domain. Cyber training and education will be significantly self-directed, modular, open-loop, and lifelong.

There is general consensus that the most significant dimension of cyber **material** is the 'software' vice the 'hardware.' As an increasingly pervasive Internet of Things is enabled by artificial intelligence (AI), we will enter an era of Sentient Tools, the next phase of development for computational systems, smart cities and environments, autonomous systems, and other advanced technologies. Current vulnerabilities allowed by design are correctable, and several disruptive materiel solutions may mitigate some future cyber vulnerabilities.

Future Commanders must be as adept at deploying cyber effects as they are at delivering physical effects. Their **leadership and education** must address desirable attributes and skills, and be broad enough to enable their ability to conceptualize rapidly and develop creative, feasible solutions to complex challenges.

Competition for talent in the cyber field will be fierce, and promises to upend our most cherished **personnel** assumptions about recruitment and retention. Motivators extend beyond monetary compensation to include patriotism, an interesting problem space, and the desire to make an impact.

Because of their ubiquitous nature and transformational characteristics, cyber infrastructure **facility** impacts on the future of conflict will be exponential vice merely additive. The centralization trend of some cyber technologies positions these central facilities as high pay-off targets that may be difficult to repair or replace.

The consequences and visibility of key cyber **policy** issues like data privacy and security, surveillance, and internet management have grown and are addressed at levels far above the Army; these policies nonetheless directly impact Army preparation for and execution of cyber operations. With most policy and precedents relatively immature, their evolution out to 2050 will be extensive.

Cyber Futures

"Cyber-casting" is problematic, but a series of **attributes** describe that elusive future:

Ubiquity. Cyber will be "everywhere" and so pervasive that in the future "cyber is no longer cyber."

Volatility. The pervasiveness and leverage of cyberspace structure will likely have a destabilizing impact on global – and local – stability.

Uncertainty. The explicit mechanism of connectivity and "cause-and-effect" in cyberspace infrastructure will be buried in the sheer mass of users, nodes, connections and data within it.

Complexity. With "cause-and-effect" relationships not readily apparent, the quantity of those relationships will shift a "complicated" system into the "complex" category.

Convergence. As data and digitization continue to move beyond information and technology communication to all aspects of our physical, cognitive and social experiences, a dominant attribute of the cyber future will be convergence.

Five potential **alternative cyber futures** define the range of potential cyber domain environments out to 2050. They include:

"Status Quo." Cyberspace conflict tomorrow looks like that of today: there are high levels of crime and espionage, but no massive cyber wars.

"Conflict Domain." Cyberspace has a range of human conflict, just like air, land, space and maritime domains.

"Balkanization." Cyberspace breaks down into national fiefdoms: there is no single internet, just a collection of national internets.

"Paradise." Cyberspace is an overwhelmingly secure place, where espionage, warfare, and crime are extremely difficult.

"Cybergeddon." Cyberspace, always un-ruled and unruly, has become a "failed state" in a near-permanent state of disruption.

Several **risky assumptions** shape our evaluation of the cyber future, to include …

… that this threat is not existential;

… that large nation-state competitors would never explicitly resort to destructive cyber warfare;

… that boundaries and authorities matter;

… that we must allocate time and energy to determining each Service's role in the cyber domain;

… that it's OK to accept software that we know is fundamentally inadequate.

Cyber's potential identity **extinction** may not be as important as cyber's impact on **human evolution**, as we increasingly recognize the impact of extended information technology exposure: cognitive off-loading, reduced memory capacity, and altered aptitude for deep learning.

Cyber Change Management

A future **vision** for the Cyber Army of 2050 must account for the relentless ubiquity and pervasiveness of cyberspace and feature the *unity of cyberspace*.

Culture modification will be a key foundation for effective change, and must take into account the disparate values and biases of successive generational cohorts including Baby Boomers, Gen Xers, Millennials, and their successors.

A sense of **ownership** will be essential to successful cyber change management, but if cyber is so ubiquitous and pervasive, who will own it? Who should?

Although most of cyber security is currently risk management, there will be an increasing need to shift the balance between **risk management and innovation** toward innovation.

Successful change management will not occur without a **sense of urgency**. Successful leaders will be the ones who create and sustain that sense of urgency, and are willing to own and address the responsibilities of a new dimension of the battlefield.

Future Learning Options

Our understanding of cross and multi-domain effects must include the cyber domain and be incorporated across the **Campaign of Learning** and then explored and validated in the numerous events that constitute **Army Force 2025 Maneuvers**.

The Army may wish to consider an extended program to develop the **future cyber operational environment by wargaming as series of alternative cyber futures** that present a range of fundamentally and substantively different cyber environments.

As the Army works to enable the creation of a cyber workforce capable of understanding the military implications of cyberspace, it must explore how talent management and cyber-partner development can address the distinct **generational learning** requirements associated with the cultural dynamics of unique generational cohorts like “millennials,” “post-millennials,” and whatever society names those born after 2020.

Cyber innovation will continue to introduce computational and cognitive tools that may accelerate shortened attention spans and memory, with significant impact on both education and learning, but also on innovation and initiative on the battlefield itself. The Army may wish to better understand the impact of extended technology exposure on Soldier performance with respect to, for example, emotional intelligence, reduced memory capacity and altered aptitude for deep learning.

In an environment featuring widespread cloud computing, machine to machine communications, artificial intelligence, and battle management applications, **operational learning** must address how cyber maneuver takes place and how commanders can arrange Army functions in time and space to meld cyber with the other domains purposefully and effectively.

Institutional learning must address life-long, open-loop learning models and assess the proper balance between training, education and certifications.

A key future learning option will be to ***define*** **cyber readiness** in a manner that is rigorous and representative of the state of the force.

Contents

Introduction: the 2050 Cyber Army

Mad Scientist (MS) is a Training and Doctrine Command G-2 (Intelligence) initiative that explores a series of future Army challenges through an open, public dialogue with a broad range of Joint, interagency and international partners; academia; policy institutions; and the private sector. Mad Scientist events are part of the G-2's continuous study of the future Operational Environment out to 2050, as well as the Army Capabilities Integration Center (ARCIC) Campaign of Learning and 2025 Maneuvers.

In September of 2016 the TRADOC G-2 and the Army Cyber Institute at the United States Military Academy cosponsored a Mad Scientist Conference called *The 2050 Cyber Army.* The 2050 Cyber Army will have a key role to play in defending Department of Defense (DoD) networks, systems, and information; defending the United States and its interests against cyber attacks of significant consequence; and providing integrated cyber capabilities to support military operations and contingency plans.[1] Proficiency in cyberspace and mastery of its relationship to the legacy domains will be a critical element of future Joint warfighting. Dominance on the land will very likely require dominance – or at minimum, extensive competitive advantage – within the cyber domain.[2]

The 2050 Cyber Army initiative is designed to visualize the Army's Cyber Force in 2050. Although this Mad Scientist project encompassed a wide range of cyber domain topics, its focus was to better understand what the Army may need to do to build the cyber workforce and develop partnerships in order to address DoD missions in cyberspace in the 2050 time frame.[3] The challenge of looking as far into the future as 2050 is daunting for any topic, and the particular nature of cyberspace compounds the already difficult task of forecasting. The technologies and capabilities that make up the 2050 Cyber Army will be defined and underpinned by sciences; technologies; cultural factors; and international and national laws, rules, and norms that are neither readily evident nor easily discernible to us today.

However, effective foresight – the process of thinking about our world and how it might change – is critical to yielding better judgments about how to best prepare for whatever the future may bring.[4] It is the intent of this study to paint a picture of key issues for the Army at the intersection of cyberspace and landpower to assist Army leaders in mapping out key decisions and actions needed to defend the Nation in and through this emerging warfighting domain.

Mad Scientist 2050 Cyber Army Conference

The Mad Scientist Conference "The 2050 Cyber Army" was held at the United States Military Academy, West Point New York from 13-14 September 2016 to explore three questions designed to illuminate the major objectives of the *Army Cyberspace Strategy for Unified Land Operations*:[5]

1. What does the cyber environment look like in 2040-2050 (how will cyber influence the environment and the population? What will connecting look like / what will they connect to? What are the drivers influencing this or not)?
2. How do we build an Army Cyber Force that can dominate the cyber domain in the context of the multi-domain battle concept to gain a position of relative advantage?
3. How can we build shared goals and expectations as well as develop an understanding of roles and responsibilities in order to build and maintain partnerships with U.S., and international academia, industry, defense departments/ministries and other agencies to enhance cyberspace operations? What new ideas should we be considering?

The conference included presentations by 10 speakers and 6 panels with 23 individual participants, including the United States Military Academy Superintendent LTG Robert Caslen, MG Malcolm Frost, Chief of Public Affairs, United States Army, BG (P) Patricia Frost, Director of Cyber, United States Army, and Mr. Thomas Greco, TRADOC DCS for Intelligence.

Conference presentations are listed at Appendix A-3 and are accessible at the following link: https://community.apan.org/wg/tradoc-g2/mad-scientist/m/the_2050_cyber_army. Notes from speaker presentations and panel discussions are synthesized into this Technical Report.

Mad Scientist 2050 Cyber Army Technology Survey

An online technology survey (available at https://survey.max.gov/818145) captured input on capability and technology ideas that could impact cyberspace and the United States Army out to 2050. Contributors were asked to provide a title and description of their capability / technology idea and to describe their idea across multiple categories, specifically: the eight TRADOC S&T Lines of Effort, six TRADOC Technology Imperatives, and the twenty Army Warfighting Challenges. (See Appendix C: Survey Results)

Mad Scientist 2050 Cyber Army Submitted Papers

Prior to the conference TRADOC G-2 issued a call for papers to address the project research questions. Six papers submitted in response were reviewed for synthesis into this report. (See Appendix A-4 for list of papers, contributors, and synopses.)

Study Context

The 2050 Cyber Army is the most recent of a series of key Mad Scientist* events. Others over the last several months have included:

- **Disruptive Technologies.** Co-hosted by Georgetown University, addressed sentient data, internet of sustainable energy, platform mergers, autonomous vs unmanned systems, and the next revolution in computing
- **Human Dimension**. Co-hosted by Army University, explored measuring cognitive potential, man-machine interface, genome sequencing, wearables, continuous diagnostics, and performance enhancers
- **Megacities and Dense Urban Areas**. Co-hosted by Arizona State University, explored the modeling of megacities, population-centric intelligence, invisible geography, hot zone robotics, avatars in the field, and the role of augmented and virtual reality in training for operations in dense urban areas.
- **Strategic Security Environment in 2025 and Beyond.** Co-hosted by Georgetown University, explored the thesis that the direction of global trends shaping the future Operational Environment (2030-2050), and the geopolitical situation that results from it, will lead to fundamental change in the character of war.

*** For the remainder of this Technical Report, the term "Mad Scientist" will connote any Mad Scientist conference presenter or participant, survey contributor, or submitted paper author for the Mad Scientist 2050 Cyber Army project.**

In addition, the analysts drew on multiple sources relevant to the conditions and consequences of future warfare and the evolution of cyberspace, including:

- The recent JCS J7 study: **Joint Operating Environment 2035: The Joint Force in a Disordered and Contested World** (14 July 2016)
- The U.S. Army's strategy paper: **The Army Cyberspace Strategy for Unified Land Operations (**January 2016)
- U.S. Army Cyber Command / Second Army White Paper: **The U.S. Army Landcyber White Paper 2018-2030** (9 September 2013)

- **United States Army Cyber Center of Excellence's Strategic Plan** (September 2015)
- Other references as cited in Appendix E to this report.

Cyberspace, War, and the Future Cyber Army

Cyberspace is defined by both the Army and the Joint community as a global domain[6] within the information environment that consists of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[7] The economic and social utility of cyberspace – as well as the significant vulnerability that U.S. and allied dependence on cyberspace entails -- places the cyber domain at the very center of our strategic thinking. This is particularly the case for the United States Army, which must not only consider the strategic and institutional implications of cyberspace for conflict, but must adapt and evolve itself in order to protect the Nation. This evolution must be based on a well founded understanding of how cyberpower and landpower relate and how unique Army capabilities can contribute to the defense of the Nation.

It is true that conflict and war are evolving and changing – and that the Army must always adapt to this change. But cyberspace is profoundly different from what has come before, exacerbating the adaptation challenge and precipitating a wide range of reactions and responses. With respect to deterrence strategies, for example, Martin Libicki has noted that "*The medium is fraught with ambiguities about who attacked and why, about what they achieved and whether they can do so again. Something that works today may not work tomorrow (indeed, precisely because it did work today). Thus, deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace*."[8] In this view, cyberspace is its own domain and conflict in cyberspace will play out according to its own unique rules and logic.

At the opposite range of response, some would argue that cyberspace is so fundamentally different than what has come before that the idea of cyber warfare itself is nonsensical. One should not try to understand competition within cyberspace in terms of war because it does not involve a physical act of violence, nor does involve force or the physical capacity to kill.[9] In this view, competitive behaviors in cyberspace may include theft, subversion, or espionage -- but will never rise to the category of war or warfare.

Either one of these perception bookends might be true if cyber effects were confined to a single domain. *The cyber domain, however, is inextricably linked to nearly every aspect of modern society.* Cyberspace literally connects a vast array of people, ideas, computers and machines through the information environment.[10] This ability to connect is changing relationships between governments, governments and the governed and between individuals themselves. Where human beings interact – particularly in new and unfamiliar ways – conflict and war inevitably follow. In fact, today's international system is marked by a fierce competition among states to define and credibly protect sovereign prerogatives in and through the cyber domain, and this contest to shape the rules in and uses of cyberspace is expected to play out for some time.[11]

As the United States and others struggle to define and credibly protect their sovereignty in cyberspace, they will conduct a wide range of military cyber operations to achieve objectives in or through cyberspace.[12] Because the cyber domain intersects throughout the land, maritime, air and space domains, cyber action is itself an integral part of military operations in all domains. The pervasive connection between cyberspace and the other warfighting domains will leverage the outcome of our future cyber competitions.

> ***"The first shots of the next actual war will likely be fired in cyberspace and likely with devastating effect."***
>
> **GEN Mark Milley,**
> **Army Chief of Staff**
> **ARCYBER Change of Command**
> **14 October 2016**

Because conflict and war in and through cyberspace will play out differently than in all other domains, the Army's institutional and operational adaptation between today and 2050 must fundamentally evolve as well. These changes must continue to posture the Army to defend DoD networks and the United States and its interests against cyber attacks of significant consequence, while being able to provide cyber capabilities to support military operations and contingency plans.[13]

This Mad Scientist report groups the outcomes of the examination of the 2050 Cyber Army along multiple themes:

Cyber Challenges: the unique characteristics of this man-made domain

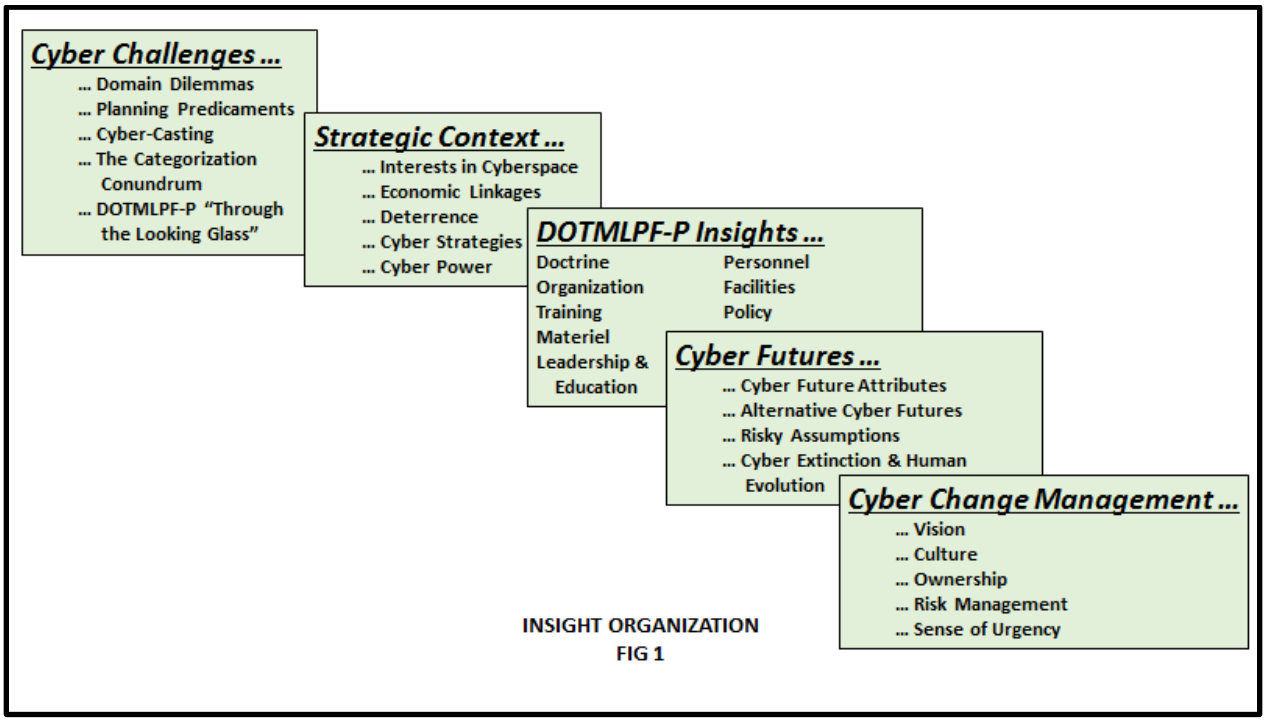
Strategic Context: how military activities and interests in cyberspace must be aligned with other national, economic, and international interests.

DOTMLPF-P[14] Insights: challenges the Army's capability development model will have to address in the cyber domain.

Cyber Futures: the need to explore and account for a range of alternative futures and consider more dangerous or less likely futures that may occur in an uncertain and fast-changing cyber environment.

Cyber Change Management: Finally, Mad Scientists addressed critical issues of institutional and cultural change in the Army to ensure it builds and maintains the capacity to defend the cyber interests of the Nation.

These major themes provided the overall organizing construct to arrange and organize the numerous observations and insights developed over the course of the project. Each were further developed in detail to provide the core structure of the 2050 Cyber Army Technical Report as shown below in Figure 1.



INSIGHT ORGANIZATION
FIG 1

The next five sections of this report will explore the 2050 Cyber Army observations and insights in greater detail along these five major thematic areas. Subsequently, the report will explore Future Learning Options prior to the Summary and Conclusion.

Cyber Challenges …

… Domain Dilemmas
… Planning Predicaments
… Cyber-Casting
… The Categorization Conundrum
… DOTMLPF-P "Through the Looking Glass"

Cyber Challenges

Domain Dilemmas

As the newest declared domain in military doctrine, the cyber domain presents multiple challenges for those who would characterize its role in military operations. It is, as GEN Michael V. Hayden pointed out,[15] the first declared domain to be a construct of man. Although the controversy behind the domain designation is institutionally behind us, there is broad recognition that the cyber domain is both significant – and fundamentally different. These domain distinctions are a common theme of cyber research.

> *"Like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, cyber. It trips off the tongue, and frankly I have found the concept liberating when I think about operationalizing this domain. But the other domains are natural, created by God, and this one is the creation of man. Man can actually change this geography, and anything that happens there actually creates a change in someone's physical space. Are these differences important enough for us to rethink our doctrine?"*
>
> **General Michael V. Hayden, USAF, Retired**

The physics of time and space in the cyber domain, for example, can generate unique and distinct considerations with respect to range, location and speed. Because of the broad interconnectivity of cyber infrastructure, the cyber domain features tactical and operational effects at global distances. Cyber effects can have global reach and effortlessly cross geographic boundaries, altering our normal perceptions of distance, proximity, and sovereignty. The notion of "position" – central to maneuver – is mostly metaphorical in the cyber domain. Homeland capabilities – being more connected – may be more at risk than "forward," deployed forces. Cyber effects can be near-simultaneous, but speed still matters: small differences in detection time, processing time, and reaction time can have huge impacts. Consequential decision cycles can be

very rapid, driving key components of the command decision process toward human-machine solution approaches.

Cyberspace, moreover, is a warfighting domain without explicit physical violence or clear attribution: cyber effects are not overtly violent and are difficult to attribute with any degree of certainty. Accordingly, their use does not trip the traditional criteria for interstate war. This state of ambiguity makes them more – rather than less – relevant for adversaries in pursuit of "gray zone" strategies.[16]

> ***" …what makes cyber warfare a potential game changer for modern conflict is the connection that states have built between digital capabilities and conventional warfare. These connections create lucrative cyber targets that impact conventional military effectiveness."***
>
> **Jacquelyn Schneider**
> **Digitally Enabled Warfare: the Capability-Vulnerability Paradox**

Cyber effects are far from limited to the cyber domain: "indirect effects" may be more significant than direct cause and effect relationships. Many would argue that the more significant effects of cyber are manifest not in the cyber domain, but through its enabling impacts on conventional, non-cyber capabilities in the other, legacy warfighting domains.[17]

Planning Predicaments

> ***"The Army has successively developed different frameworks for visualizing the commander's area of operations (AO) in terms of places, people, and things. A virtual dimension has emerged that requires reconciliation with the physical and cognitive dimensions for commanders to define and operate in their respective Operational Environments."***
>
> **The U.S. Army Landcyber White Paper, 2018-2030**

Although the cyber domain is a human construct, the complexity of cyber infrastructure, together with the speed and global reach of cyber action, frustrates the ability to "visualize" cyber-space in a coherent way.[18] Visualization – a process central to our approach to Mission Command – is problematic in a domain where action is often not directly observable, and can happen at discrete points far below the platform level.

Terrain, a key factor of consideration in the military planning process, is clearly a somewhat metaphorical idea in cyberspace, but that metaphor is stretched by more than the man-made origins of the cyber domain. Cyber "terrain" – to the extent that it can be visualized – is not a set of enduring features that shape maneuver such as

> ***"Everyone concedes that cyberspace is man-made … it is not the man-made nature of cyberspace that makes it different. Cities are man-made, but city combat shares many of the rules of country combat. What matters is that cyberspace is highly malleable … in ways other media are not."***
>
> **Martin C. Libicki**
> **"Cyberspace is Not a Warfighting Domain"**

in other domains. It does shape maneuver, to be sure, but this "terrain" is highly malleable by human action, both friendly and adversarial.[19]

A clear majority of the "volume" that constitutes cyberspace, moreover, is not well mapped, existing as the "Deep Web" and "Dark Web" and constitutes terrain that frustrates exploration and exploitation without special skills and permissions.[20] This "slo-go" (deep) and "no-go" (dark) cyber terrain is estimated by some to be more than 500 times the size of the Surface Web.[21] Attempts at cyber visualization will be problematic if we can't see ourselves, threats, and all of the relevant cyber "terrain."

The domain dilemmas of cyberspace pose daunting challenges for the intelligence function in planning. The cyber domain, with rapid changes in technology and the adaptive behavior of attackers, defenders and users, is not a system where historical data is always a useful predictor of outcomes. For systems that are not isolated, stationary, and recurrent, collecting more information does not equate to having more knowledge.[22] Many cyber intelligence tools are therefore only forensic in nature. Accordingly, current cyber intelligence is typically made available to decision makers "after the fact" vice "before the fact."

Planning is further complicated by an asymmetry of defensive and offensive planning authorities. For the United States, reaction (and defense) is decentralized; action (and offense) tends to be highly centralized. The offense / defense dynamic is also asymmetric to our state and non-state adversaries, who – unlike us -- frequently decentralize both offensive and defensive operations.

Cyber-Casting

Extending one of the major themes described in the Mad Scientist *Strategic Security Environment* project, the rate of change in cyber science frustrates forecasting of the future state of the cyber domain. Indeed, attempting to forecast the nature of the cyber domain in the year 2050 is akin to projecting the nature of our current cyber environment in 1982: one year before the birth of the internet. Taking into account the ever-accelerating rate of change in the cyber domain, the cyber-casting challenge is even more daunting.

The ability of DoD to anticipate developments in the cyber domain will probably not improve. DoD was originally a key driver in the realm of cyber capability development, with dominant roles in landmark cyber innovations such as the internet, Central Processing Units (CPUs), Random Access Memory (RAM), Packet Switch Networks, and Transmission Control Protocol / Internet Protocol (TCP / IP) networking protocols. That leading role is now significantly diminished and dispersed among state and non-state entities. The military will not regain its dominant influence on cyber developments, limiting the ability of the DoD to shape its general architecture and direction.[23]

Ten years forward is regarded as an ambitious forecast in the cyber realm. One Mad Scientist participant, futurist Brian David Johnson, suggested that forecasts must be multidisciplinary, incorporate "gates" to alert us to decision points where we can shape the desired future, and "flags" to confirm or deny our forecasts. Such a forecast can incorporate successive horizons including:[24]

- Social science for nearest term events
- Technology feasibility estimates for pending developments
- General trends that describe the "math" of the future
- "Data with an opinion" – discussions with informed individuals
- "Science fiction" prototypes.

Cyber forecasting / threat-casting is at best a framework for understanding – vice prediction -- "so that when something does happen, we are prepared" … the goal of the process is to 'get it right,' not 'be right.'[25]

We form military theories and strategies in the hopes of gaining some anticipatory, predictive benefit from those intellectual frameworks, but the unique characteristics of the cyber domain frustrate their predictive power. Battle results are indirect, not readily observable, and difficult to quantify. Feedback loops are fragmented, and although the OODA framework is generally operative, actors are anonymous, and engagements happen at machine speed.[26] Predicting cyber outcomes is even problematic in the near term.

The Categorization Conundrum

The ubiquity and pervasiveness of the cyber domain positions it as a broad link that bridges the physical, cognitive, and moral dimensions of conflict. Cyberspace actions can cause physical impacts, alter our available information and understanding, and even -- through information warfare – influence the moral dimension (the dimension of belief). This broad range of relevance is both a blessing and a curse: underscoring the utility of cyberspace action while presenting endless opportunities for categorization confusion as cyber emerges as a disparate aspect of every institution and process.

The categorization conundrum is manifest in many ways as the institution positions this capability for the future. Some would advocate centralization of cyber capabilities for efficiencies and control; others advocate that this key enabler must be distributed and aligned to legacy capabilities. Cyber has a profound "boundary busting" impact that diffuses the distinctions between civil and military action, between the physical / informational / moral dimensions of conflict, and across the diplomatic, informational, military, and economic (DIME) elements of power. In the Army we see this boundary

ambiguity in the overall convergence of *Electronic Warfare*, *Signal*, *Information Operations*, *Intelligence*, *Public Affairs*, and of course: *Cyber Operations*.[27]

DOTMLPF-P "Through the Looking Glass"

Collectively, the cyber challenges generate an "alternative domain" environment where our experiences are – as Alice in Wonderland would declare -- "curiouser and curiouser!" Although the DOTMLPF-P model is still applicable – and will be applied in this report -- a quick preview of the model illustrates that in every aspect the cyber domain lives up to its reputation as a domain that is both significant and different:

> ***"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that."***
>
> **The Queen of Hearts**
> **"Alice in Wonderland"**

Doctrine: What does "doctrine" mean when the highest form of cyber art is the unprecedented, "zero-day" attack: an exploitation of the unknown vice the application of principles?

Organization: How do organizations account for the fact that technology is simultaneously both *centralizing* (e.g., cloud computing) and *decentralizing* (e.g. device to device (D2D) communications in the Internet of Things (IoT)?

Training: How will any training system address the fact that cyber technologies will advance several cycles over the duration of a typical military career?

Material: Can an industrial age acquisition system accommodate "material" concerns where the most relevant "system" is typically at the sub-platform level; the most significant part of that system is "software" vice "hardware"; and "open-sourced software" is considered more effective than "closed-sourced?"[28]

Leadership and Education**:** What is the role of leaders (and their education) when they will rarely be the most technically competent (or relevantly experienced) member of their organization?

People**:** Can our legacy personnel policies deal with technology impacts that include significant alteration of our very processes of cognition?

Facilities**:** How do we plan for cyber infrastructure considerations that are global and external to military and perhaps even national control?

Policy**:** How will the Army shape governing policy that typically originates and is decided outside of its decision purview?

This Page Intentionally Left Blank

Strategic Context …

… Interests in Cyberspace
… Economic Linkages
… Deterrence
… Cyber Strategies
… Cyber Power

Strategic Context

Interests in Cyberspace

Because of the ubiquity of the impacts of digitization, our interests in cyberspace are generally congruent to national interests, but with influences (and impacts) that are more global, reflecting the world-wide interconnectivity of cyber infrastructure. There is little indication that these interests will substantively change out to 2050. They include:[29] [30] [31]

- The protection of vital assets, such as critical infrastructure, civilian government agencies, and key private sector entities from cyberattacks from both state and non-state actors.
- The reasonable resistance and resilience of U.S. physical and cyber infrastructure to concerted, sophisticated cyber-attacks – both destructive and disruptive.
- That the United States maintains a technological lead in key information technologies, particularly military-related technologies.
- Preservation of a level playing field for international trade and finance.
- Collective cyber defense in partnership with key U.S. allies.
- That the United States maintains its strong position in international distribution of information so that American ideals of freedom, security and prosperity continue to influence positively the cultures of other nations.
- Preservation and expansion of the ability of citizens everywhere to access information and engage freely in political speech.
- Preservation of the privacy of individual citizens and the security of classified information.
- Definition and protection of compatible international rules and norms in cyberspace that encourage stability and regular economic relations among states.

The United States commitment to open, interoperable, and reliable cyber communications enables prosperity, public safety, the free flow of commerce and ideas -- and reflects the core American values of freedom of expression and privacy, creativity, opportunity, and innovation. In yet another illustration of the paradoxical nature of the cyber domain, however, this very commitment to ready communication and agile data flows simultaneously provides dangerous state and non-state actors opportunities to undermine U.S. interests while advancing their own.[32]

Economic Linkages

Both the National Security Strategy[33] and the most recent Quadrennial Review recognize a strong American economy as the "foundation of U.S. power."[34] Although some believe that existing economic measures do not capture it adequately, all agree that the digital economy is growing rapidly, and in the United States and around the globe this economy is more resilient and faster-growing than the economy as a whole.[35] The cyber domain and the digital economy at work within that domain will be an increasingly vital element of this strength.[36]

> ***"Accenture models "the digital economy" … at a total value of $5.9 trillion amounting to 33 percent of U.S. GDP in 2016."***
>
> **Cameron F. Kerry**
> **Bridging the Internet-Cyber Gap: Digital Policy Lessons for the Next Administration**

Because of its ubiquity and pervasiveness, digitization and cyber technologies, like electricity, are general-purpose technologies that underpin a growing share of economic activity beyond the information technology sector that supplies them.[37] Most nation-states are adopting strategies aimed at improving their digital competitiveness by expanding infrastructure, developing e-government, and directly promoting digital industries.[38]

The Snowden incident illustrates that the linkages between our strategic economic and security interests within the cyber domain are quite direct. The Snowden fallout tarnished America's national reputation as well as the brands of a number of American companies. The Snowden event also generated increased pressure for national data localization laws requiring that data about individuals within a country be kept in that country, for restrictions on transfers of data from the European Union, and for shifting internet governance away from the loose collection of organizations involved today toward intergovernmental bodies such as the United Nations.

Some authoritarian and non-Western governments don't need the shock of a Snowden-like provocation to emulate the Chinese model of "digital sovereignty" by leveraging increasingly available blocking and surveillance capabilities, insisting on data localization, and requiring local information technology manufacturing. Authoritarian pressures, taken together with democratic data sovereignty concerns, cast some doubt on whether the "world-wide web" will continue to expand as a global commons or

whether it will fracture into a set of national or regional networks.[39] These two potential outcomes will have very divergent impacts on the nature of our cyber future.

Finally, the digital / cyber economy presents significant challenges to economic equality and the future of work. The cyber economy relies on relatively few people (as opposed to mass industrialization), and cyber innovation and globalization is a poster child for the risks of massive social and economic dislocation associated with new technologies. An accelerating and growing gap in income and mobility can undermine growth, opportunity, and the social fabric, bringing the economic impacts of the cyber domain to the surface of political concern and increasingly under the purview of senior government decision makers.[40]

Deterrence

A key strategic consideration out to 2050 will be the future role of deterrence in the cyber domain. Expensive and wide-ranging defensive cyber efforts – such as firewalls, virus detection, and network monitoring are the current focus for protection of the integrity of U.S. cyber systems. However, a range of cross- and multi-domain deterrence tools are emerging that may include sanctions, indictments, cyber retaliatory options, and even the threat of kinetic measures in response to cyber provocations.[41] The ubiquity of cyberspace weapons and the difficulty of attribution in cyberspace, however, means that our traditional deterrence options will not always succeed against a variety of cyber threats – state or non-state – in the future.[42] [43] Cyber attackers are hard to identify with certainty, and even if identified the evidence frequently cannot be made public. The counterstrike, if there is one, is equally hard to discern and – if covert – has limited impact as a publicized, future deterrent.[44]

> ***"The problem is not with deterrence theory, or with cyberweapons' offensive utility, but that too many people are trying to peel off the bumper-sticker version of complicated Cold War debates on deterrence and apply them to a more complicated present and future."***
>
> **Peter Singer**
> **"How the United States can Win the Cyber War of the Future" (2015)**

Deterrence is further hard to establish because there are no international treaties or norms about the use of digital weapons by states, non-state groups or individuals – or even acknowledgment by the U.S. Government that it has ever used them itself. There are effectively no rules to constrain cyber conflict other than perhaps those – general guidelines such as proportionality – that bound warfare in general.[45] There is little consensus about how the laws of war may apply in cyberspace and the development of international norms, standards and laws will take decades, as will an intellectual and doctrinal framework to integrate cyber response coupled with a demonstrated record of US government capacity, readiness, and willingness to respond to provocation.

Peter Singer and other cyber theorists have argued that the cyber domain frustrates almost every attempt to apply Cold War deterrence models. They argue that future deterrence efforts should include the establishment of norms, fleshing out a mutual understanding of the "new rules of the game": each side must understand that its opponent will continue to conduct cyber-activities ranging from espionage to theft. The most important goal is not to stop every cyber attack, but to keep them from escalating into something far more dangerous. They further suggest "deterrence through diversity," positing a range of potential reactions that can be significantly delayed in time, target third parties of interest, or occur far outside the cyber domain. Most significantly, they forecast that cyber deterrence will be most effectively centered on "deterrence by denial" — making attacks less probable by reducing their likely value. Cyber resilience -- the demonstrated capacity to continue operating through an attack and recover rapidly -- can limit the gains accruing to an attacker.[46]

The US Government published its policy on cyber deterrence in 2015, advocating a two-pronged approach that includes "deterrence by denial" and "deterrence by cost imposition." The deterrence by denial approach encompasses defense, resiliency, and reconstitution initiatives to provide critical networks with a greater capability to prevent or minimize the impact of attacks; together with strong partnerships with the private sector to promote cybersecurity best practices, assist in building public confidence in cybersecurity measures, and lend credibility to national efforts to increase network resiliency. The "deterrence by cost imposition" line of effort includes, but is not limited to: pursuing law enforcement measures; sanctioning malicious cyber actors; conducting offensive and defensive cyber operations; projecting power through air, land, sea, and space; and, after exhausting all available options, to use military force.[47]

Cyber Strategies

The Army's challenges within the cyber domain are but a subset of the strategic challenges encountered by all the services, the entire government, and in fact our entire society. Army approaches to future cyber conflict, therefore, must take into account the context of a broad, multi-echeloned array of cyber strategies; these will evolve many times between now and 2050, but their current status is worthy of a quick review:

- The White House **International Strategy for Cyberspace** is a synthesis of U.S. concerns in the digital arena aimed explicitly at "engagement with international partners on the full range of cyber issues." It weaves together technical principles (interoperability, stability, reliable access, and security) with values (freedom, respect for property, privacy, and protection from crime) and governance (multi-stakeholder institutions, and self-defense).[48]

- The **DoD Cyber Strategy**[49] focuses on building cyber capabilities and organizations for DoD's three primary cyber missions: to defend DoD networks, systems, and information; defend the Nation against cyberattacks of significant consequence; and provide cyber support to operational and contingency plans. The strategy sets five strategic goals:
    - Build and maintain ready forces and capabilities to conduct cyberspace operations;
    - Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
    - Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
    - Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages; and,
    - Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Within the Army, two significant documents address the strategic context for the future of the Cyber Army:

- The **Army Cyberspace Strategy for Unified Land Operations in 2025** seeks to integrate cyber forces, capabilities, facilities, and partnerships to execute Joint and Army operations and to support the DoD strategy along five Lines of Effort:
    - LoE 1: Build the Workforce
    - LoE 2: (Offensive / Defensive) Operations
    - LoE 3: Capability Development
    - LoE 4: Facilities, Systems and Infrastructure
    - LoE 5: Partnerships

- The **Army Cyber Center of Excellence Strategy** pursues a vision of a highly-skilled workforce that effectively collaborates with relevant stakeholders to develop and lead integrated cyber, signal, and electronic warfare and signal solutions (capabilities) for the Army and Joint Forces. It's five Lines of Effort include:
    - LoE 1: Transform the Army Cyber Center of Excellence and Ft Gordon
    - LoE 2: Develop the Cyber Workforce & Leadeship
    - LoE 3: Develop Army Entrerprise Concepts, Doctrine and Requirements
    - LoE 4: Champion Cyber Integration
    - LoE 5: Develop a Sustainable Resource Strategy

Both Mad Scientists and other outside sources have noted that the Electronic Warfare function – particularly its relationship to the cyber domain -- lacks a coherent vision and strategy at both DoD and Army levels.[50] [51] [52]

> *"It is important to lay down a marker with the Russians. They have gone too far and need to be checked. The U.S. needs to navigate a narrow and difficult path between inaction and escalation. We can start by recognizing that this is cyber conflict, not the kind of cyber conflict we planned for but a conflict nonetheless. Anything we do should reinforce (or at least not undercut) the long-term goal to create a framework of agreements for stability in cyberspace. The U.S. also needs a larger strategy for dealing with Russia and its new style of conflict that uses hybrid warfare against some opponents and a mix of cyber actions, disinformation, and corruption against others."*
>
> **James Lewis**
> **thecipherbrief.com**

The presence or absence of documentation, however, will not be the determinant factor in the assessment of cyber strategy adequacy. During the preparation of this analysis, at least two significant cyber events captured public attention in the United States. The hacking of the Democratic National Committee was tentatively attributed by the US Government to the Russians. At about the same time, one of the largest Distributed Denial of Service (DDOS) attacks ever observed struck several public domain servers, leveraging a large infrastructure of inadequately secured devices in the Internet of Things. The public outcry over these attacks has included assessment that our cyber strategies remain far from adequate.[53]

Cyber Power

> *"If a foreign country went and bombed a Johnson & Johnson plant in our country, it would be viewed as an act of war. If someone makes Johnson & Johnson go dark, the world yawns … no one comes to the rescue of a Fortune 50 Company … and the law says we can't fight back."*
>
> **Marene Allison, CISO**
> **Johnson & Johnson**
> **Mad Scientist Conference: the 2050 Cyber Army**

As for the legacy domains, our capabilities in the cyber domain will ultimately render strategic consequences. To practice effective mission command, sustain the forces, provide critical intelligence, and communicate over the horizon, a nation must -- of necessity -- be a cyber power.[54] Cyber power will not, however, ensure cyber sovereignty: the cyber domain exhibits a "sovereignty gap," wherein the Government cannot protect the private sector against all relevant threats. The challenge of cybersecurity, therefore, may increasingly be one of civil defense: how to equip the private sector to protect its own computer systems in the absence of decisive government involvement.[55]

Cyber power will not, moreover, always accrue to those nation states that are well positioned in the more classical dimensions of power. The "barriers to entry" for those who would acquire cyber capabilities is relatively low. This opens the door to cyber power status to both weaker nations as well as non-state actors. Strategic cyberwar theory views adversarial nations as comprehensive frameworks of institutional arrangements instead of merely a set of military assets and digital networks. These institutional frameworks are likely to be less well defended than the industrial-military complex. However, when influenced, subverted or attacked, these frameworks can have an outsized impact on an adversary. Leveraged in this way, cyber action can diminish the underpinnings of an adversarial regime.[56]

> ***"Cyberpower, in particular, is tailor-made for a country in Russia's circumstances – a declining economy with the gross domestic product of Italy. It is dirt cheap, hard to trace to a specific aggressor and perfect for sowing confusion, which may be the limits of Mr. Putin's goals."***
>
> **Peter Sanger**
> **New York Times**

Cyber power presents national decision makers with a destabilizing capability / vulnerability paradox. The greater the reliance on advanced cyber capabilities – both as direct weapons and as enablers for conventional capabilities – the greater the potential disruption, diversion, and destruction that adversaries can create via malicious cyber activities in the future. This situation motivates both stronger and lesser powers toward preemptive action: the stronger in order to preserve their advantages; the lesser in order to mitigate their disadvantages.[57] The most capable and least risky future military may be one in which digital technologies enhance capabilities but are not uniquely critical vulnerabilities.[58]

> ***" … the F-22 is primarily designed to gain air superiority against cutting-edge enemy aircraft; the kind of fight the U.S. has not actually faced in decades. Similarly, cyber warfare must be considered not only in the context in which it is currently utilized, but in how it could and would be utilized in wars in the future. We must anticipate and prepare for total cyber war."***
>
> **Alexander McCoy**
> **Best Defense Blog, 18 March 2015**

Most importantly, it would be imprudent to view the future impact of cyber power as a linear extension of its role today. This technology frequently advances in a non-linear pattern; its application in warfare could be similarly non-linear. Careful strategic anticipation and preparation will be warranted.[59]

This Page Intentionally Left Blank

DOTMLPF-P Insights …

Doctrine	**Leadership & Education**
Organization	**Personnel**
Training	**Facilities**
Materiel	**Policy**

DOTMLPF-P Insights

Doctrine

Doctrine typically draws from theory, but with respect to cyber, future doctrine confronts several theoretical challenges.[60] Although cyber serves as a bridge between the physical, the cognitive, and the moral dimensions of conflict, there is no broadly accepted or dominant theory that simultaneously addresses these multiple conflict dimensions. This leaves doctrine with relatively weak and disputed theoretical underpinnings for categorization, principles, and similar tools of doctrine. Much of our current theory, for example, was derived from the industrial age and is built on physical metaphors (e.g., centers of gravity) with little relevance in the cyber domain, where the "physics" of time and space are distinct from the legacy domains that shaped our current doctrine.

Doctrine must illustrate cyberspace as a warfighting domain, portraying operations across the land, air, and space domains that will occur by, with, and through the cyber domain.[61] The cyber domain, however, is a relatively new field that will continue to be reshaped on an almost daily basis by emerging technical capabilities – and threats. The growth of cyber capabilities so far has outpaced the development of relevant theory and doctrine. Doctrinal "levels of war," for example, pose unique challenges in the cyber domain. In the cyber domain, tactical actions routinely have global reach, and significant "sub-platform warfare" at the computer chip or software level can either be isolated to singular platforms or pervasively damage entire lower-layer infrastructures like Operating Systems (OSs), hardware, hard drives, and memory disks -- thereby crippling widespread capabilities and services that depend on these lower layers.[62] There will be an institutional and operational imperative to doctrinally define maneuver in cyberspace,[63] but in the absence of physical "position," schematics for maneuver in cyber are highly complex and dynamic, defined by ever-changing avenues of approach that include routers, switches, bridges, and servers that provide data transfer, routing, and storage instructions for the data packets.[64] Nonetheless, Commanders will recognize the fundamentals of maneuver warfare as equally applicable in cyberspace:

targeting critical vulnerabilities; audacity; surprise; focus; decentralized decision-making; tempo.[65] Although reaction and after-the-fact forensics are dominant in current cyber operations, the Army will seek to extend its historical doctrinal imperative to seize, maintain and exploit the initiative to the cyber domain.[66]

> ***"Mastery of classic combined arms principles is a must, but the advent of new technologies and the rising importance of virtual domains like space and cyber are evolving the relationship among Soldiers, machines, and software. As the character of war is about to undergo a fundamental change, both the operating force and the institutional Army likewise look fundamentally different as we develop and sustain new forms of maneuver, mass, and mutual support."***
>
> **GEN Mark Milley**
> **CSA, US Army**
> **Army.mil, 4 October 2016**

The Army will also retain its doctrinal focus on combined arms integration; the challenge will be to both plan and incorporate cyberspace capabilities into the commander's scheme of maneuver. Doctrine must facilitate the coordination and synchronization of organic intelligence assets and nonlethal effects in support of the commander's objectives through the targeting process. That process itself will evolve with increasing threat and the U.S. use of the cyberspace domain and the electromagnetic spectrum (EMS).[67] The Army currently projects four Mission Areas to integrate across cyber-electromagnetic activities (CEMA), inform and influence activities (IIA), and Joint Information Operations (IO):[68]

- **Force Enhancement**: Create and transfer knowledge by the networks and information systems that create the Common Operating Picture.
- **Support**: Build a defensible network.
- **Force Application**: Exploit, attack, and influence capabilities to deliver effects in and through cyberspace.
- **Control**: Provide freedom and maneuver and action within Army networks and network systems.

With a wider array of tools available to directly alter enemy perceptions and understanding, one probable doctrinal trend out to 2050 will be the elevation of deception in our doctrine. No longer an ancillary benefit, deception will be a routine feature – and frequently a primary purpose – of cyber operations. Because of the pervasiveness and ubiquity of cyber activity, deconfliction will be a daunting combined arms challenge, including deconfliction not only of activity but also of purpose.[69] A common deconfliction challenge will be the tension between options to *disable* vice *monitor* enemy cyber capabilities.

> ***"In the course of "ratcheting" up cyber-attacks on ISIL there has been open discord and disagreements between the Intelligence Community (IC) and Cyber Command over whether to disable or monitor ISIL operations. If discord exists in the disabling or monitoring question now, wouldn't these disagreements intensify in 2040-2050 near peer competitor fight, with thousands of potential cyber targets?"***
>
> **CPT Kurtis M. Hout**
> **Submitted Paper, Mad Scientist: the 2050 Cyber Army**

Organization

New unit types are the traditional solution approach for integration of new technology capabilities into the combined arms team, and that process is well underway with the DoD formation of the Cyber Mission Force. This force is composed of four types of teams: 68 Cyber Protection Teams to defend priority DoD networks and systems against significant threats; 13 National Mission Teams to defend the United States and its interests against cyberattacks of significant consequence; 27 Combat Mission Teams to provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations; and 25 Support Teams to provide analytic and planning support to the National Mission and Combat Mission Teams.[70]

The Army contribution to the Cyber Mission Force comprises 41 teams, and the Army has centralized its cyber planning and development capabilities by stationing ARCYBER Headquarters and the Joint Force Headquarters-Cyber at Fort Gordon, Georgia near the National Security Agency's Georgia facility. Other major decisions included establishing the Cyber Center of Excellence (Cyber COE) at Fort Gordon and transferring cyber proponency from ARCYBER to the Cyber COE. The centralization at Fort Gordon as the Army's center for cyberspace operations is an initiative to increase the Army's unity of effort and command within this warfighting domain.[71]

> ***"Cyber/Electromagnetic Activity needs to get buy-in from the brigade … we automatically want to create another stovepipe called CEMA, segregating the cyber specialists into their own isolated domain, but that's a bad bureaucratic habit. Cyber and electronic warfare need to be integrated with everything — artillery fire, ground maneuver, logistics — in a single coherent plan. And that integration has to be the commander's job …"***
>
> **COL Jerry Turner**
> **Commder, 2d SBCT**

The 41 Army CMTs have a strategic role as part of the ARCYBER support to CYBER Command's National Mission Force to support DoD Networks. At the tactical level the Cyber Support to Corps & Below (CSCB) effort is exploring ways to support individual Army corps, divisions, and brigades.[72] For every efficiency and control advantage gained from centralization and specialization, there will ultimately be an associated integration challenge to generate combined arms effects. These integration requirements will span the Army combined arms team, the Joint Team, the interagency, and the multinational force. The convergence of time and space, technology and functional synergy increasingly will compel the Army to find ways to seamlessly integrate and unify the operational and institutional force as well, enabling operational force reach back to the institutional force to solve fast-paced, emerging problem sets.[73]

The Reserve components may prove to be particularly well suited to augment Army cyberspace requirements. At the strategic level, reserves can contribute specific strategic multidiscipline analysis to support the preparation of the Operational Environment. At the operational level, the Reserve component may increase the size of units and add EW, IO, leader engagement, and MI functionality to improve existing capabilities.[74]

In the cyber domain, the Army's future organizational solutions must account for technology trends that are simultaneously both centralizing and decentralizing: Unprecedented centralized virtual communications networking technologies like Software Defined Networks (SDNs) and virtualized clouds coexist with completely distributed ad hoc mobile networking (MANET) and device to device (D2D) networking architectures.[75] Because of the cross-boundary ubiquity and reach of cyber operations, moreover, fixed organizational solutions alone will not suffice.

Organizational solutions in the cyber domain will typically include extensive use of inter-disciplinary – and inter-organizational -- teaming and partnering. The role of partnerships was a dominant theme in this Mad Scientist project, which highlighted the need to think differently about partnerships. Inter-service, inter-agency and international organizations are all interconnected and their relationships become more complex at every level. Industry, academia and government, and private-public partnerships will need to come together in a "Center for Disease Control" approach to prepare, prevent, respond and recover to meet today's and tomorrow's most challenging problems.[76]

The Army's potential partners will approach future relationships with caution, viewing the military culture as reliant on directive authority vice collaboration.[77] Successful partnership endeavors, therefore, will impose a premium on cross-institutional transparency, trust building, and collaboration**.** The Federal Acquisition Regulation (FAR), lamentably, is currently not optimized to accommodate this type of organizational approach.[78]

> ***"I think you have to look at this as the first step in a journey that may, over time, lead to the decision to break out Cyber the way … the Army Air Corps became the U.S. Air Force, the way Special Operations Command was created, although that still has service parts to it."***
>
> **SecDef Ashton Carter**
> **23 March 2015**

The organizational dimension of future cyber solutions promises to be an enduring issue, at least for the near term. Now that cyber is a declared domain, proposals for a Cyber Service are inevitable.[79] Advocates for such a solution will argue that if cyber attacks will constitute future acts of war, then our cyber defenses and countermeasures must be under the constitutional limitations governing the use of military force, and control of our cyber power should migrate from its current concentration in law enforcement and intelligence agencies.[80] Moreover, a Cyber Service – with appropriate statutory and regulatory foundations -- could optimize recruiting standards and service "organize, train

and equip" responsibilities for the unique attributes of the cyber domain. Others will suggest that each legacy warfighting service should optimize its cyber capability to reflect the needs of their own domains – and culture – and that portions of these capabilities could evolve to a very consolidated unified command such as SOCOM.[81] They will argue that because this function is an aspect of virtually every activity of modern warfare, integration of yet another centralized service would exacerbate combined arms synergy challenges. The ultimate outcome of this debate will have significant impacts on combined arms integration and capability development from both a material and human capital perspective.

Training

For legacy DOTMLPF-P analysis, professional education is generally associated with leader development; in the cyber domain, such education will be inseparable from training.[82] [83] Cyber warriors are "knowledge workers" and as such they need more than "training;" they need a strong education in cyber fundamentals in order to enable an understanding of the complexity of the cyber domain.[84] [85] The effective lifespan of a technical cyber degree, however, is about three years.[86] Continuous learning, therefore, either self-directed or on-the-job, will be a routine feature of future cyber training and education.

Essential cybersecurity job requirements also include soft (non-technical) skills, specifically: leadership, communications ability, and interpersonal skills, as well as problem-solving, influencing, and relationship building.[87] Thus while higher education may not be able to keep up with rapidly changing technology, it can provide a solid foundation for emerging cybersecurity professionals.[88]

> *" … the value of certs in cybersecurity is relatively unique. "This is materially different from other professions, where folks are compelled to maintain some level of currency by continuing education credits," Reeder says. "Cyber ninjas see certifications as being effective … in maintaining their currency."*
>
> **Kelly Jackson Higgins**
> **"The Keven Durant Effect: What Skilled Cyber Security Pros Want"**

In the cyber domain, however, education and training are not enough. The cyber field has a very strong emphasis on technical certifications in critical skills such as cybersecurity tools, information security, and network engineering.[89] Although certifications are emerging as one of the most important dimensions of cyber training, accelerating changes in technology might threaten the

> *"Education will increasingly be fully envisaged as a life-long experience, rather than a one-shot, four year stint. The Stanford team's idea, called "The Open Loop University," will entail "six years of non-linear residential learning" so that students drop in and out of the on-campus experience during their lifetime to join a diverse, fluid community of learners."*
>
> **Margaret Andrews**
> **StratEDgy Blog**

currency of certifications.[90] Here, as for education and training, the solution will be a life-long approach to learning (and certification) in the cyber domain.

Mad Scientist Conference participants generally agreed that cybersecurity is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, mathematics, physics, political science, engineering, sociology, decision sciences, international relations, ethics and law.[91] Cyber education must not only be multi-disciplinary, it must extend outside of the classroom environment.[92] Such an idea is congruent with recent views that higher education will increasingly become "open-loop" experiences, focusing more on problem-solving competencies in multi-disciplinary teams vice individual, single discipline mastery. Cyber training and education will be significantly self-directed, modular, open-loop, and lifelong.[93] [94]

Individual cyber skills will be a concern not only within Cyber Mission Force units, but across the combined arms team: as cyber technology becomes ubiquitous, so too must a fundamental set of cyber skills. These skills can no longer be relegated to IT organizations.[95] With respect to collective training, Mad Scientists advocated incorporation of cyber capabilities into large scale training exercises in order to establish credibility with the broader operational force.[96] At both the individual and the collective level, future training can leverage simulation or gaming technology, aided by artificial intelligence that replicates real terrain, physical structures, and social interaction in cyberspace.[97]

> ***"Don't assume you have to train future generations the way we were trained; that is the height of hubris … the younger generation has completely different experiences: it's 'Minecraft' versus 'Pong.' Understand their mindset."***
>
> **Scott Stevenson**
> **Mad Scientist Conference: the 2050 Cyber Army**

Mad Scientist Conference participants encouraged the audience to not underestimate the unique dimensions of training developments in the cyber domain.[98] In the words of LTG(R) Rhett Hernandez: "The pyramid is upside down." The school system will worry less about how graduates stay in touch with educational updates, and more about how the school can stay in touch with what is happening in the field. Younger Soldiers in the formation may frequently be more technically current than senior leaders. Cyber technologies, moreover, will continue to accelerate the process of 'cognitive off-loading' in humans, whereby computational / cognitive tools shorten our attention spans and memory.[99] The impacts on future training and learning will inevitably be profound.

Material

The ubiquity, pervasiveness, and acceleration of cyber technology change poses daunting challenges for 'materiel' cyber capability development, even to the point of stretching our current understanding of 'materiel.' There is general consensus that the most significant dimension of cyber tools is the 'software' vice the 'hardware.' From game-changing weapons to routine back-office systems, the DoD is entirely reliant on its ability to identify, acquire, certify, deploy, and manage software.[100] It seeks to address this challenge with an Industrial Age acquisition system that pre-dates the very idea of software.

Software is both the driver of cyber capability as well as the locus of most cyber vulnerabilities. It is also relatively 'dynamic' compared to legacy materiel considerations, in that it is frequently and routinely altered – ideally through upgrade improvements, but unfortunately sometimes by adversary action. It will merit the examination of alternative acquisition approaches. Some will argue that – counterintuitively – "open source" software development models are generally better than their proprietary counterparts because they can take advantage of the brainpower of larger teams, which leads to faster innovation, higher quality, and superior security for a fraction of the cost.[101] Others will question the security liabilities of such an approach, although in many cases increased public scrutiny of code has led to identification and reconciliation of problems that were not discovered through "closed" quality checks.[102]

The concurrent trends of cyber material decentralization (Internet of Things (IoT), Device to Device (D2D) computing) and centralization (cloud computing) have the unfortunate consequence of simultaneously vastly expanding the cyber system 'attack surface' while also enhancing the payoff to cyber attacker for controlling of critical software functions.[103] The Department of Defense and the Army will be a component of this connectivity trend. An echelon's tactical operations center or local security command post, for example, will operate intelligent arrays: intelligent networked capabilities that provide visual, signature, or movement warning for local security and perimeter defense.[104] The number of devices connected to the Army network at the tactical edge will continue to grow and empower leaders and warfighting formations. However, these devices are often wireless and commercial off-the-shelf, thus introducing added protection risk. Proper use, accountability, configuration, and management of these devices will be critical to effective Army operations.[105]

Innovative sight, sound, and touch technologies are making cyber computing increasingly pervasive, driving the next wave of innovative cyber computing in private, commercial, public, and warfighter networks.[106] Mad Scientist participant Brian David Johnson has suggested that as the Internet of Things is married to artificial intelligence, we will enter an era of Sentient Tools. Sentient Tools are "what comes next" and will emerge from a base of computational, sensing and communications technologies that have been advancing for over the last 50 years. Sentient Tools will drive the next phase

of development of computational systems, smart cities and environments, autonomous systems, artificial intelligence, big data and data mining, and an interconnected Internet of Things (IoT). They will have four components:[107]

- **Situational Awareness:** Sensing the outside world via local and networked sensors as well as data and expertise sharing
- **Intelligence:** Processing, understanding, learning, making sense of the world
- **Social Awareness:** Understanding who it is engaging
- **Communication:** The ability to communicate with the human (multimodal interactions e.g. voice, visuals, audio, haptic, etc.)

> ***"Current after-the-fact forensic approaches such as virus checkers are like running a background check on the hobos living in your bedroom."***
>
> **Panel: "Community of Hackers and Makers and Innovative Thinkers" Mad Scientist Conference: the 2050 Cyber Army**

Some observers note that the impact of the emerging Internet of Things, including Sentient Tools, can portend colossal chain reactions of damage to connected systems unless we reform our generally undisciplined approach to cyber design. There are incorrect perceptions that security and innovation are antithetical; we will need secure components for building codes; and must look earlier in the design cycle to build foundationally more secure systems.[108] An end-to-end security architecture starting at the basic nano, micro, and macro hardware-level along with thread-level of software is feasible,[109] and although many of our current security vulnerabilities are by design; over time many of these design flaws can be corrected.[110] [111]

Mad Scientist contributors also took note of a long-known but frequently overlooked risk: electromagnetic pulse (EMP) vulnerabilities. Near-peer competitors like Russia, China, North Korea, and Iran all make EMP attack a complementary part of their cyber doctrine. Our increasing dependence on advanced electronics systems results in the potential for an increased EMP vulnerability of our technologically advanced forces, and if left unaddressed, makes EMP employment by an adversary an attractive asymmetric option.[112]

Several disruptive materiel solutions may mitigate some future cyber vulnerabilities:

- Quantum sensing and quantum communication may eliminate the vulnerability of radio frequency (RF) transmission to eavesdropping, information manipulation or information spoofing.
- Read-Only Memory (ROM) reduces the vulnerability of a piece of software to accidental or malicious modification.

- For supply chain management, split fabrication of integrated circuits provides a disruptive paradigm to reduce the risk of malicious backdoors in hardware, at significantly lower cost and higher potential success than detection.[113]
- There are promising, alternative future security models that mimic biological systems to trace end-to-end system calls for both data and control flow messages differentiating whether a given common library or any other asset has been accessed by an authentic authorized system calls of "immunized" systems (termed as "self") or by adversarial system calls (termed as "non-self") with nearly 100% probability for both known and unknown attacks.[114]
- Complexity of the signal environment might be addressed by autonomy to figure out counter-measures including "self-healing" that work at machine speed and far surpass any potential human reaction range.[115] [116]

Although there is a current assessment that with respect to cyber materiel developments the offense is generally "ascendant," the potential disruption of these technologies on that trend could fundamentally alter the course of our cyber futures.

Leadership and Education

To paraphrase Leon Trotsky, "*Some of you Leaders may not be interested in cyber warfare, but cyber warfare is interested in you*." Future Commanders must be just as adept deploying cyber effects as they are delivering physical effects.[117]

Desirable attributes and skills of future cyber leaders was a common theme throughout the Mad Scientist Conference. Those attributes and skills are summarized in the table below.[118] [119]

Desirable Future Cyber Leader Attributes	Desirable Future Leader Skills
• Sense of Urgency • Inquisitiveness: Look at things not from "what is" but what "could be" • Discontent with the Status Quo • Determination: Never Giving Up • Adaptability to Change • Resilience • Self-awareness of strengths and weaknesses • Creativity • Risk Tolerance • Ambiguity Tolerance	• Mission acumen • Technical ability to understand the threat – and to know, recognize and call "BS" • Team building • Relationship building • Recognition of the Big Picture • Change Management • Strategy articulation • Empowerment • Influence (without direction authority)

As indicated in these lists of skills and attributes, technical competency is only a subset of the requirement for cyber leaders. Future cyber leader education must broaden their abilities to conceptualize rapidly and develop creative, feasible solutions to complex challenges. Conflicts in cyberspace will also require a profound understanding of foreign culture, foreign languages, intelligence capabilities, use of diplomatic means, Army foreign area operations, cyberspace operations, and civil affairs operations.[120] They must be able to succinctly convey complicated cyberspace conceptual or analytical material in a manner that is understood clearly by decision-makers.[121]

There will be a war for talent, particularly cyber leaders, across our society. The Army must think now about how to motivate and retain its most effective cyber leaders.[122] Empowerment will be a key tool – not only to acquire and retain talented leaders, but also as a leadership competency. In the coming age of pervasive autonomy, this critical function of empowerment will extend beyond subordinates to machines: pre-authorized responses will be developed by humans, but executed at machine speed.[123] Decision-making, the essence of a leader's command and control process, will increasingly be shared with *sentient tools* like artificial intelligence.

Personnel

Individuals and their behavior are typically the "weak link" in cyber engagements,[124] in fact, insider threats typically do more damage to cyber capabilities (and to institutions) than external adversaries. Personnel considerations, therefore, will be significant not only for the future cyber force but for the Army's success as a whole in the cyber domain. For the Army of 2050, as cyber becomes ever more entwined with the fabric of our systems and our institutions, every Soldier will be a "Cyber Warrior**."**[125]

The fundamentals for Cyber Warriors will include passion, critical thinking, and problem-solving.[126] Competition for such talent in the cyber field will be fierce, and promises to upend some of our most cherished assumptions about recruitment and retention. Many individuals are in the cyber components of the military because of patriotism, an interesting problem space, and the desire to make an impact.[127] Although a competitive salary is a threshold requirement, employment discriminators beyond pay include interesting work and the ability to hone their skills alongside talented colleagues. 46% profess relative disinterest in promotion to management positions, preferring to remain hands-on with

> ***"It's not just about the money: skilled cybersecurity professionals most value a position that includes challenging work with plenty of variety, training and career development, and where they work alongside similarly highly-skilled security pros."***
>
> **Kelly Jackson Higgins**
> **"The Keven Durant Effect: What Skilled Cyber Security Pros Want"**

respect to coveted security skills including threat analytics, advanced forensics, intrusion analysis, secure programming, and penetration testing.[128]

The recruiting process, moreover, must effectively begin earlier. Mad Scientist participants opined that to get ready for 2050, the Army needs to stop recruiting at shopping malls. Instead, it should recruit at STEM programs; find young people with cyber aptitude in middle and high school and develop relationships that support and encourage youth to bring their cyber skills to service in the Army.[129] One of the best ways to enhance cyber recruiting, therefore, will be to lower the barrier of understanding between the US population and their government / military.[130] The source of power for the Army is the American people: their trust and confidence, their financial resources, and most importantly, their sons and daughters. At the Mad Scientist conference MG Malcom Frost described a distinct civilian-military drift: the American people only see us through the lens of warfare: Iraq and Afghanistan. They do not understand that Soldiers are driven, skilled, educated. We are at a strategic communications inflection point; the American people are about to "move on."[131]

> *"I think everybody can agree that we can't build and retain a cyber force like we have done traditionally with other aspects of the force."*
>
> **Army Secretary Eric Fanning**
> **24 Oct 2016**

Mad Scientists believed that money will not be nearly as useful for retention of future cyber talent as empowerment.[132] A sense of purpose, therefore, may be the most effective recruiting tool.[133] [134] In addition, fundamentally altered career models may be effective. The Army (and Navy) offer direct commissions to dentists and doctors, why not for cyber talent?[135] There could be a revolving door that works in both directions: cyber professionals could routinely transfer between DoD and private industry, to the significant benefit of both employers.[136]

Facilities

Like so many other aspects of the DOTMLPF-P model, the facilities dimension poses unique considerations in the cyber domain, considerations that go well beyond the brick, mortar, power systems and computers we associate with cyber facilities. The cyber domain is itself a man-made, globalized infrastructure of capabilities and vulnerabilities that connects to a family of weapons and platforms. In that sense, the advancements that cyber technologies bring to modern conflict may be more akin to the impact of roads, railroads, or combustion engines than to the rifle, the tank, or the aircraft carrier. Digital technologies are integrated into every domain, across weapon systems, and across all levels of warfare. Because of their ubiquitous nature and transformational characteristics, both the capabilities and the vulnerabilities this cyber infrastructure imbue will be exponential as opposed to merely additive.[137]

Although cyber actions can occur at machine speed and the technology can advance very rapidly, some aspects of the cyber domain infrastructure such as cell tower systems, fibre-optic cable or satellite constellations require years if not decades of anticipation, planning and investment. The centralization trend of some cyber technologies such as cloud computing positions those central facilities as high pay-off, significant targets for either cyber or kinetic attack – facilities that may be difficult to repair or replace. Over-centralization of facilities may impede *resilience* – a highly desirabe attribute for effective cyber deterrence.

Policy

Because cyber infrastructure is simultaneously a delivery mechanism for both the economic and social benefits of information and communication technology, as well as weaponized cyber threats, policy stakeholders include both "*internet* optimists" and "*cyber* pessimists." These two groups have alternative perspectives on cyber domain opportunities and threats. Bridging the "internet-cyber" gap will be a conundrum for current and future policy makers and will emerge as a continuous challenge to policy optimization for Army and Joint operations:[138] the Army, like the other services, is far from master of its own fate with respect to cyber policy. The consequences and visibility of key cyber issues like data privacy and security, surveillance, and internet management have grown and are addressed at decision levels above the Army; in many cases: by the President.[139] Those policies nonetheless directly impact Army preparation for and execution of cyber operations.

> ***"U.S. deterrence policy currently has the feeling of roulette. Maybe the house still wins overall, but it is clear that actors like Russia are happy to keep spinning the wheel while they're ahead."***
>
> **Susan Hennessy**
> **Brookings Institute**

Some issues of cyber policy will migrate to the level of constitutional issues, for example: Presidential Policy Directive (PPD) 20 authorizes the United States government to counterattack state-sponsored hackers who target America from overseas. However, no act of Congress authorizes or rejects Presidential Policy Directive 20. Because an execution of PPD 20 could cause collateral damage to domestic computer networks, some believe that Supreme Court balance-of-powers precedents[140] might call into question the constitutionality of any cyberattack the President orders as domestic, rather than foreign policy.[141]

On the time scale of constitutional and legal precedent, the cyber domain is in its infancy; its legal and policy foundation will evolve significantly from now to 2050. The "Law of Cyber Warfare," for example, is not yet established. The North Atlantic Treaty expressly states the right to collective defense in the face of "armed conflict" but lacks language accounting for cyber warfare.[142] Automated cyber engagements may require

rethinking legacy Title 10 and Title 50 boundaries.[143] The issue of enabling "civil defense" in the cyber domain is problematic, with some positing the possibility of "letters of marque,"[144] or "cyber Blackwaters."[145] Others warn of dire consequences if authority for pre-emptive or counter-offensive action is delegated to the civilian sector.[146]

> ***"A private can shoot someone, but to "shoot" electrons needs a 3- or 4-star approval."***
>
> **Audience Question to Scott Weaver, Defense Digital Service Mad Scientist Conference: the 2050 Cyber Army**

The constraints and restraints of policy already impact cyber operations and will continue to do so in the future. Mad Scientist participants noted that authorities have the negative impact of keeping commanders from training on missions they are not currently authorized to execute.[147] The evolution of policy for decision authorities has not kept pace with technology advances in the cyber domain. Conference participants believed that as cyber engagements proliferate, the policy will inevitably evolve "because it has to."[148] Some of our most important future cyber capabilities, such as digital resiliency, will not be possible without an effective policy foundation that underwrites modular, decentralized, redundant capabilities as legitimate requirements in spite of their increased costs.[149]

This Page Intentionally Left Blank

Cyber Futures …

… Cyber Future Attributes
… Alternative Cyber Futures
… Risky Assumptions
… Cyber Extinction & Human Evolution

Cyber Futures

Cyber Future Attributes

The challenges of "cyber-casting" explored in earlier sections of this report impose a shroud of uncertainty around the cyber future out to 2050, but Mad Scientists described a series of consistent attributes about that elusive future:

***Ubiquity*.** Cyber will be "everywhere" and so pervasive that in the future "cyber is no longer cyber."[150] The functional distinction of things "cyber" will diminish as cyberspace connectivity (e.g., the Internet of Things) pervades every aspect of our infrastructure.[151] From a military perspective, the pervasiveness of cyberspace will challenge the Army to reconceptualize time and space across all of the domains – including cyberspace -- to win future battles and wars.[152]

***Volatility*.** The pervasiveness and leverage of cyberspace infrastructure will likely have a destabilizing impact on global – and local – stability. Digitization and social media, for example, will blend "weaponized data" and potentially micro-target anyone on the planet.[153] The multiplicity of potential actors – and the expansion of the means at their disposal – can only be problematic for a stable operational environment.

***Uncertainty*.** The explicit mechanism of connectivity and "cause-and-effect" in cyberspace infrastructure will be buried in the sheer mass of users, nodes, connections and data within it. Increasing portions of cyberspace action, moreover, may be shaped through artificial intelligence tools and machine to machine communications, without direct human oversight or review. A destabilization of certainty and trust is inevitable as foundational data and fundamental algorithms powering the Internet of Things are attacked and inexplicably fail.[154] Vulnerabilities at the fringes of the global supply chain, moreover, will present weak links in the cyber infrastructure, posing doubt about the reliability and assured performance of cyberspace infrastructure.[155]

***Complexity*.** Cause-and-effect relationships in the cyber domain will not be readily apparent, and the quantity of these relationships will shift merely "complicated" systems into the "complex" category. Blended attacks originating from every aspect of cyberspace ubiquity will present new levels of complexity.[156] Very complex automated systems across the Internet of Things, moreover, will present an immense and vulnerable attack surface. The more efficient these systems become, the easier they will be to hack.[157] Simplicity will be a limited virtue, frequently defeated by creativity and flexibility. Adversaries may steal ideas from an attacker's playbook, for example, as a useful tool against targets of their own.[158]

***Convergence*.** Data and digitization continue to move beyond information and technology communication to all aspects of our physical, cognitive, and social experiences.[159] The consequent attribute of the cyber future will be *convergence* **…**[160]

> **…** between land and cyberspace operations.
> … between all the legacy domains, as cyberspace constitutes the connective ether that readily transfers effects from one domain to another.
> **…** between time and space as enhanced information and communication technologies decrease the time and expand the reach of cyber actions.
> … between electromagnetic (EMS) and cyberspace action.
> … between defensive and offensive cyberspace operations to ensure one function informs the other.
> … between information management (IM) and knowledge management (KM) as large data is leveraged to achieve advantage.
> … between Army operational and institutional activities, creating an unprecedented level of interaction where operations impact institutional activities and vice-versa.

Alternative Cyber Futures

Given the uncertainty associated with cyber-casting, a useful approach for evaluating the future out to 2050 is to describe a range of alternative futures and attempt to identify key discriminators that distinguish between them. Although that was not an explicit task of the Mad Scientist Conference, in a project for the Atlantic Council Cyber Statecraft Initiative, Jason Healy identified five alternative cyber futures describing a range of conflict and collaboration.[161] Since Mad Scientist discussions touched on most of these potential outcomes, we leverage that analysis in this report.

The potential alternative futures are as follows:[162]

> **"Status Quo."** Cyberspace conflict tomorrow looks like that of today: there are high levels of crime and espionage, but no massive interstate cyber warfare.
>
> **"Conflict Domain."** Cyberspace reflects a wide range of human conflict, just like air, land, space and maritime domains.
>
> **"Balkanization."** Cyberspace breaks down into national fiefdoms: there is no single internet, just a collection of closely guarded and poorly interconnected national internets.
>
> **"Paradise."** Social and technological innovations make cyberspace an overwhelmingly secure place, where espionage, warfare, and crime are extremely difficult.
>
> **"Cybergeddon."** Cyberspace, always un-ruled and unruly, has become a "failed state" in a near-permanent state of disruption, including high levels of hacker, criminal, and terrorist activity.

The key discriminator that drives alternative cyber futures in this model is the technology contest outcome between offensive and defensive cyber operations. The impact of relative primacy between offense and defense on these alternative futures – together with prospects for conflict and collaboration – are summarized in the following table.[163]

	Status Quo	Conflict Domain	Balkanization	Paradise	Cybergeddon
Description	Cyberspace conflict tomorrow looks like that of today: there are high levels of crime and espionage, but no massive cyber wars.	Cyberspace has a range of human conflict, just like air, land, space, and maritime domains.	Cyberspace has broken into national fiefdoms: there is no single Internet, just a collection of national Internets.	Cyberspace is an overwhelmingly secure place, as espionage, warfare, and crime are extremely difficult	Cyberspace, always un-ruled and unruly, has become a "failed state" in a near-permanent state of disruption.
Relationship of Offense and Defense	**Offense** > Defense	**Offense** > Defense	Unknown/Depends	**Defense** >> Offense	**Offense** >> Defense
Intensity and Kind of Conflict	Conflict is as it is today: bad, but not catastrophic, with crime and spying.	There is a full range of conflict: crime, spying, embargos, and full-blown international conflict.	Nations are possibly blocking access to content, to and from each other, although there may be fewer outright attacks.	All conflict is greatly reduced, although nations and other advanced actors retain some capability.	Every kind of conflict is not just possible, but ongoing, all of the time.

Intensity and Kind of Cooperation	There is a healthy but limited sharing on response, standards, and cyber crime.	To be stable, cyber cooperation requires norms and regimes, just as in other domains.	Cyber cooperation requires international agreement in order to interconnect national Internets.	Cooperation is critical if stability depends on norms, or unneeded if it depends on new technology.	Cooperation is either useless, as attackers always have the edge, or impossible, like trying to govern a failed state.
Stability	Relatively Stable	Relatively Stable?	Unknown/Depends	Long-Term Stable	Long-Term Unstable
Likelihood	Moderate	High	Low	Low	Low
Why This Is Possible	Current trend line and massive attacks have not occurred yet, despite fifteen years of expectations.	Other domains have generally supported a range of human activity, from commerce to conflict.	Countries continue to build border firewalls, which UN control of the Internet could exacerbate.	New technologies or cooperation, long promised, could make security much easier.	Offense continues to outpace defense, as any new defensive technology or cooperation is quickly overcome.

The current assessment of cyber offense ascendancy in the Mad Scientist Conference would reinforce Jason Healy's estimate that the "Conflict Domain" outcome is currently most likely. Recent actions by authoritarian regimes to attempt to control internet access and other uses of cyberspace – together with concerns that the cyber domain as currently constructed and managed is simply too vulnerable and dangerous – argue for a "Balkanization" outcome. Only if the disruptive material solutions previously described[164] substantially mitigate future cyber vulnerabilities will the "Paradise" outcome be feasible.

Risky Assumptions

Mad Scientist panel participants were invited to identify implicit assumptions that shape our current evaluation of the cyber future, particularly dangerous ones. The principal themes that emerged included …[165]

> **… that this threat is not existential**. Many still don't see cyber as an existential threat but for many industries already today it is exactly that. Intellectual property theft happens every day, and for an increasing number of individuals, moreover, the majority of their "existence" is within the cyber domain.
>
> … **that large nation-state competitors would never explicitly resort to destructive cyber warfare**. Several Mad Scientists dismissed the theory that interdependence will eliminate the risk of cyber war with emerging peer competitors. Relative gains might prove irresistibly attractive to such a

competitor, and a cyber actor less reliant on – and less able to leverage the cyber domain – might wish to level the playing field.

… **that boundaries and authorities matter**. We will not be able to rely on our internally conceived boundaries and authority limitations to secure the Nation when the enemy doesn't care about how we delineate the problem – unless it is to use those artificial distinctions to their own advantage.

… **that we must allocate a lot of time and energy determining each Service's role in the cyber domain.** Allocation of roles (based on legacy boundaries and responsibility assignments) takes us down a path that is not tenable. In a domain that is notoriously "cross-boundary," we will be better served to identify opportunities for partnership, collaboration, and unity of effort.

… **that it's OK to accept software that we know is fundamentally inadequate**. The assumption that software deficiencies are inevitable and an unavoidable consequence of market forces is unwarranted and should not be acceptable. Companies seek the fastest time to market and then try to clean up the mess afterwards. In the words of the Mad Scientist Panel Community of Hackers and Makers and Innovative Thinkers: "Day-0's need to go away: we should be able to build systems that are provably secure. It's possible to write bug-free programs."[166] [167]

Cyber Extinction and Human Evolution

> ***"Cyber is no longer cyber in 10-15 years. It doesn't live in the digital anymore. It is moving to social and kinetic. The framework is getting wider."***
>
> **Brian David Johnson**
> **Mad Scientist Conference: the 2050 Cyber Army**

A final observation on the future of cyber: *does it even have one?* Several Mad Scientists surmised that by 2050 cyber will be so ubiquitous, pervasive, and integrated into every aspect of our existence that it will lose its unique functional identity.[168] Cyber's potential identity extinction, moreover, may not be as important as cyber's impact on the evolution of human identity. Science is increasingly recognizing the impact of extended technology exposure on human behavior, with a broad series of outcomes including cognitive-offloading, reduced memory capacity, and altered aptitude for deep learning. These outcomes are not per se "good," or "bad," particularly when evaluated in combination with the benefits of technology capabilities. But they are nonetheless significant factors that will over time reshape training and education, communication, and every aspect of societal interaction. Whatever the future of cyber will be, it is inextricably intertwined with our own.

This Page Intentionally Left Blank

Cyber Change Management

Vision

Change management was a recurring theme in this Mad Scientist event. A future vision for the Cyber Army of 2050, in particular, must account for the relentless ubiquity and pervasiveness of cyberspace. It must feature the *unity of cyberspace*: for the battlefield of 2050 the appropriate concepts, doctrine, relationships, and arrangements must be built jointly between industry, militaries of different countries, and inter agency partners.[169] Mad Scientist participants noted the role of vision in a simple "DVP" formula for change; where D is the level of dissatisfaction, V is the Vision, the "painted picture," and P is the path: the hardest part – the roadmap into the future.[170] They also noted the important role for *meta-cognition*: the ability to recognize the ideas we already hold.[171]

> ***"Who will be writing the cyber version of 'Eating Soup With a Knife'?"***
>
> **LTC Dan Smith, Panel Moderator**
> **Mad Scientist Conference: the 2050 Cyber Army**

Culture

Just as cyber will pervade every aspect of our future culture, so too will our current culture pervade every aspect of cyber change management. Culture modification will be a key foundation for effective change.[172] As cyber technologies have begun to shape human behavior, successive generational "cohorts" have emerged, each with distinct behavioral traits. Effective change management must account for the default culture associated with each of these cohorts. One Mad Scientist presentation suggested that the most significant current cohorts – and their defining values -- include:[173]

Baby Boomers: Respect - Baby Boomers want and believe in respect.

Generation X: Freedom - Generation X'ers want to chart their own path.

Millennials: Authenticity - Millennials want organizations to encourage, enable and value their true selves.

Change management must adapt its messaging to relate to each cohort on its own terms – and both anticipate and be sensitive to the evolving values of future cohorts.

Ownership

> *"Stop thinking of who is in and who is out in fighting the cyber war. We're all in."*
>
> Marene Allison, CISO
> Johnson & Johnson
> Mad Scientist Conference: the 2050 Cyber Army

A sense of ownership is essential to effective cyber change management, but if future cyber is ubiquitous and pervasive, who will "own it?" Who should? Mad Scientists noted that all too frequently legacy leaders are inclined to "let the S-6" address the cyber challenge.[174] Imbuing a sense of ownership – not only in commanders but in all Soldiers – will be a prerequisite for effective change management in a domain where "every Soldier is a Cyberwarrior."[175] [176] Future cyber leaders who master the key cyber leader competency of empowerment will be more successful in this task.

Risk Management and Innovation

The Army has a rich culture of risk management, but Mad Scientists foresaw an evolution in the balance between risk and innovation. Although most of cyber-security is risk management, they perceived an increasing need to integrate cultural and process solutions with technical solutions.[177] Government agencies must shift mentality from "check the box" compliance to more active risk management.[178] They assessed the current culture of the cyber security community as "20% innovation, 80% compliance": as compliance security is commoditized, the innovation dimension needs to expand.[179] A culture of innovation within the cyber community will require thinkers and leaders who are willing to …[180]

… give more than they take.
… step outside the box.
… bridge communities.
… build relationships.

Mad Scientists noted that we cannot change culture without changing process, including the very process of education. Our educational institutions will not be able to deliver creative, innovative thinking without significant cultural change themselves.[181] Pedagogy," for instance, does not work for technology innovation: students must build knowledge out of an ecology of ideas.[182]

Sense of Urgency

Several Mad Scientists agreed that – given the need to adapt our Army and culture as technology evolves -- a sense of urgency is necessary and certainly warranted.[183] Successful leaders will be the ones who create and sustain that sense of urgency, and are willing to own and address the responsibility of a new dimension of the battlefield.[184]

> ***"Senior leaders in the Department and beyond the Department understand that cyber is a problem [and] cyber is important. They've made cyber a priority, and there is a sense of urgency.,"***
>
> **MG John A. Davis**
> **July 1, 2013**

This Page Intentionally Left Blank

Future Learning Options

The many choices identified in this study present a rich set of options for the Army in its enduring responsibility to prepare for the future defense of the Nation. Some of these important choices with respect to future learning options can be further explored, understood, and acted upon across a range of Army institutional processes.

Campaign of Learning and Force 2025 Maneuvers

This report notes that conflict and war in and through cyberspace will play out differently than in all other domains. As several of the insights contained within this report illustrate, the Army Campaign of Learning must account for the pervasiveness of cyberspace and the rise of military cyber operations across all facets of the operational and institutional Army. As the domain that bridges the physical, cognitive, and moral dimensions of conflict, the Army can leverage cyber theory and doctrine to better integrate these multiple dimensions of conflict. Our understanding of cross and multi-domain effects must include the cyber domain and be incorporated across the Campaign of Learning and then explored and validated in the numerous events that constitute Army Force 2025 Maneuvers. Because the attributes and dynamics of the cyber environment change quickly, the Army must be flexible in its approach to cyber learning across the Force 2025 Maneuvers program.

Cyber-Environment Development: Wargaming Alternative Cyber Futures

One way to “design-in” mental flexibility and encourage non-conventional thinking about the future in general (and cyber operations in particular) is an “alternative futures” approach to future planning. The Army may wish consider an extended program to develop the future cyber operational environment by wargaming as series of alternative cyber futures that present a range of fundamentally and substantively different cyber environments. This report describes a wide range of potential cyber futures dependent on the outcome of core technology variables that will play out over the next few decades. Wargaming these alternate cyber futures may assist in better understanding key assumptions, actions or decision points. Moreover, a family of wargames across dramatically different cyber futures may expand the range of potential options for Army cyber integration and cyber employment out to 2050. Alternative cyber futures over a

range of wargaming events may facilitate deeper exploration of unconventional or unexpected approaches to cyberspace.

Generational Learning

The human dimension will present important issues at the intersection of generational culture and the cyber domain. In 2050 nearly everyone in the Army will be a “digital native” with a unique cyber presence. The Army will need to explore what initiative and “mission command” mean in an environment in which everyone is fully active and present in the cyber domain. As the Army works to enable the creation of a cyber workforce capable of understanding the military implications of cyberspace, it must explore how talent management and cyber-partner development can address the distinct generational learning requirements associated with the cultural dynamics of unique generational cohorts like “millennials” and “post-millennials.” Each succeeding generation will be increasingly familiar and competent in using a range of information technologies, robotic and autonomous systems, and other aspects of a highly connected and information-rich civilization. Ironically, as many of these technologies are developed and deployed commercially, they may become harder to operate and maintain from a technical perspective. User friendly hardware and software may be coded, designed, and built by very few people. People may be more familiar with pre-programmed apps rather than coding themselves. The correct mix of ‘back end’ programmers and technologists will be critical if the Army does not want to become an army of “end-users” of technologies developed and deployed by others.

Cyber Innovation and Soldier Performance

Battlefield artificial intelligence (AI), including automated engagement networks, automated decision aids, and anticipatory, self-deploying logistics packages are some of the technologies that will arrive by 2050. In this environment, everything on the battlefield will sense, communicate, and decide in some manner. While robotics and autonomous systems – all of which reside the cyber domain – take on more of the “thinking,” information technologies are encouraging a measure of ‘cognitive off-loading’ in humans. The many computational and cognitive tools (and in the future, AI and neural networks) may accelerate shortened attention spans and memory, with significant impact on both education and learning, but also on innovation and initiative on the battlefield itself. The Army may wish to better understand the impact of extended technology exposure on Soldier performance with respect to, for example, emotional intelligence, reduced memory capacity and altered aptitude for deep learning.

Operational Learning

This report has frequently noted the profound blurring of boundaries that cyberspace encourages between civil and military action, between the physical / informational / moral dimensions of conflict, and across the diplomatic, informational, military, and economic (DIME) elements of power. Understanding the operational impact these elements through the cyber domain will be critical. The Army should explore the proper level of centralizing and decentralizing decision-making with respect to cyber operations. In an environment further blurred by widespread cloud computing, machine to machine communications, artificial intelligence, and battle management applications, it will need to understand how cyber maneuver takes place and how commanders can arrange Army functions in physical time and space to meld cyber effects with the other domains purposefully and effectively.

Institutional Learning

A frequent theme in this report is the notion that by 2050 the line between "student" and "graduate" may blur, meaning that cyber professional development never ceases. Moreover, for the Army of 2050, as cyber is entwined with the world, including the full panoply of our systems and our institutions, every Soldier will in some way be a "Cyber Warrior**."** In fast moving technical areas, certifications and continuous learning may be as important as full degree programs. If the Army truly is manned by cyber warriors, these certifications must be developed and implemented – without neglecting proficiency in other core land warfare competencies. Although certifications are emerging as one of the most important dimensions of cyber training, swift technological change threatens the currency of certifications, while some advanced military cyber functions may not be found in the private, university, or technical sectors – particularly those that reside at the intersection of technical capabilities and of national security strategy and operational and tactical warfighting. The Army must understand the balance between external training and education, Army-specific cyber coursework, continuous learning, self-directed study and on-the-job training.

Defining Cyber Readiness

Although readiness is the current priority of the 2016 Army, it is a safe projection that cyber readiness will be an important priority all the way out to 2050. The most important learning requirement will be to *define* cyber readiness in a manner that is rigorous and representative of the state of the force. Partnerships will be central to a cyber-ready force because of the blurring of many of the lines described above. To be ready, the

Army may wish to investigate ways to develop and maintain a range of cyber-capable partners that will inhabit the future information environment. A cyber-ready Army must be capable of seamlessly integrating or deconflicting interests and operations among a range of potential friendly cyber actors. Cyber readiness may also require more extensive integration of the operational and institutional force as well, enabling operational force reach back to the institutional force to solve fast-paced emerging problem sets. The Army should explore a range of organizational solutions in the cyber domain, including extensive use of inter-disciplinary teaming and partnering, putting a premium on cross-institutional transparency, trust building, and collaboration, perhaps going so far as to develop “open source warfare” of fast-paced cross organizational teams capable of “programming and coding the fight” at the speed of the conflict.

Summary and Conclusion

On October 21, 2016, as analysts synthesized Mad Scientist observations for this Technical Report, a massive internet disruption occurred. Twitter, Paypal, Spotify, and other popular social networking and online payment services were virtually inactivated when Dyn, a commercial information technology company that supports the internet's domain name system (DNS) was overwhelmed by an enormous amount of traffic. This was a distributed denial-of-service attack (DDoS), perhaps of unprecedented scale. Even more interestingly, and certainly more worryingly, the attackers hijacked tens of thousands of simple "Internet of Things" devices – digital video recorders, security cameras, and internet routers – to raise a virtual cyber army of unwitting "bots" that generated enough waves of digital traffic to flood the system and bring it to a halt.[185] If you watch Netflix via a home router, you might have been a draftee in this bot cyber army.

What was this? We are uncertain. Was it an act of massive cyber vandalism or a warning message from a nation state?

Who did this? The notorious attribution challenge of the cyber domain extends to this case. Some have argued that this can only be the action of an advanced nation state; others propose that it was an exercise gone awry at the hands of amateurs.

Why did they do this? Perhaps, as analyst Bruce Schneier has suggested, this was an extended probing attack to learn more about our vulnerabilities. Perhaps it was a bored computer science major. With the actors totally invisible to us, their motivations are even more so.

How can we fix this? By removing and replacing the devices incorporated into our cyber infrastructure with no or inadequate security protections. Intel Corporation estimates there will be 200 billion of them by 2020. Those "speed to market" design trades are coming home to roost.

What will happen next? Does this portend "Cybergeddon?" Or will our institutions find policies and partnerships that address design problems like this and put us on the path to cyber "Paradise?" What might the Cyber Army of 2050's role be on that path?

Ubiquity. *Volatility*. *Uncertainty*. *Complexity*. *Convergence*. Welcome to the cyber future!

[1] GEN Mark Milley; Chief of Staff, U.S. Army The Army Cyberspace Strategy for Unified Land Operations, January 2016, pp. 2

[2] Lieutenant General Edward Cardon; Former Commander, U.S. Army Cyber Command and Second Army, "The Future of Army Maneuver – Dominance in the land and Cyber Domains" The Cyber Defense Review, pp, 16.
[3] Build the Workforce is LOE 1, Partnerships is LOE 5 in GEN Mark Milley; Chief of Staff, U.S. Army The Army Cyberspace Strategy for Unified Land Operations, January 2016, pp. i
[4] Mad Scientist Conference 2016: Strategic Security Environment in 2025 and Beyond (October 2016), pp 12-13.
[5] GEN Mark Milley; Chief of Staff, U.S. Army The Army Cyberspace Strategy for Unified Land Operations, January 2016, pp
[6] The term "domain" is not specifically defined in either Army or Joint Doctrine, however, Joint Publication 3-0 provides important context, noting that a Joint Force Commander's operational environment is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment (which includes cyberspace). Included are enemy, friendly, and neutral systems that are relevant to a specific Joint operation.
[7] Definition of cyberspace from Joint Publication 3-12 *Cyberspace Operations* and ARDP 1-02 *Terms and Military Symbols.*
[8] Martin Libicki, Cyberdeterrence and Cyberwar, *RAND (*2009), p. iii.
[9] See, for example, Thomas Rid, *Cyber War will not Take Place* (2013), or *Misconceptions about Conflict in Cyberspace*, George Marshall Institute
[10] The information environment is defined in both Army and Joint Doctrine as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information ARDP 1-02 *Terms and Military Symbols and DoD Dictionary of Military and Associated Terms*.
[11] Joint Staff J-7, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (14 July 2016), p. 34.
[12] Joint Publication 3-12 *Cyberspace Operations* and ARDP 1-02 *Terms and Military Symbols.*
[13] GEN Mark Milley; Chief of Staff, U.S. Army The Army Cyberspace Strategy for Unified Land Operations, January 2016, pp. 2.
[14] DOTMLPF-P: Doctrine, Organization, Training, Material, Leadership & Education, Personnel, Facilities, and Policy.
[15] Michael V. Hayden, The Future of Things "Cyber," 5 STRATEGIC STUD. Q. 3, 4 (2011), available at http://http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.
[16] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," International Security (Fall 2013).
[17] Jacquelyn Schneider, Digitally-Enabled Warfare: The Capability-Vulnerability Paradox, CNAS Report August 2016.
[18] *The U.S. Army Landcyber White Paper, 2018-2030*, Army Cyber Command (9 September, 2013), p. 7.
[19] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain", I/S: A Journal of Law and Policy for the Information Society, v. 8, no. 2, Fall 2012, p. 325-340, posted on 01 Jan 2012. Available at http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf.
[20] The Surface Web is anything that can be indexed by a typical search engine like Google, Bing or Yahoo; the Deep Web is anything that a search engine can't find; the Dark Web is classified as a small portion of the Deep Web that has been intentionally hidden and is inaccessible through standard web browsers. "Clearing up Confusion: Deep Web versus Dark Web." Bright Planet Blog, March 27, 2014 at https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.
[21] Zach Epstein, "How to Find the Invisible Internet," BGR.com on 20 January 2014 at http://bgr.com/2014/01/20/how-to-access-tor-silk-road-deep-web/.
[22] Robert Zager and John Zager, "Why We Will Continue to Lose the Cyber War (Response to Cyber Proficient Force 2015 and Beyond)", paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.
[23] Matt Weaver, Rogue Leader, Digital Defense Service; "Pervasive Capability: Our Only Hope", Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016
[24] Brian David Johnson, 'A Widening Attack Plain: Initial Cyber Threat-casting Report out for Mad Scientists", Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

[25] Brian David Johnson, Futurist in Residence, Arizona State University; "A Widening Attack Plain: Initial Cyber Threat-casting Report out for Mad Scientists", Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[26] Dr. Jan Kallberg, "Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* (Spring 2016).
[27] BG(P) Patricia Frost, Director of Cyber, US Army, "Opening Comments / Stage Setting" Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[28] Ben FitzGerald, Peter L. Levin, and Jacqueline Parziale, "Open Source Software and the Department of Defense", Center for A New American Security, August 2016.
[29] Authors note: this list does not attempt to distinguish between interests that are "vital," "extremely important," or "important."
[30] Graham T. Allison and Robert Blackwill, "America's National Interests: A Report from the Commission on America's National Interests" July 2000.
[31] Jeffrey A. Eisenach, Claude Barfield, James K. Glassman, Mario Loyola, Shane Tews. "An American Strategy for Cyberspace" American Enterprise Institute, June 2016.
[32] Department of Defense, "The DOD Cyber Strategy." Department of Defense, April 17, 2015.
[33] National Security Strategy, 2015.
[34] Quadrennial Defense Review, 2014.
[35] Kerry, ibid.
[36] Cameron F. Kerry, "Bridging the Internet-Cyber Gap: Digital Policy Lessons for the Next Administration," Center for Technology Innovation at Brookings, July 2016.
[37] Kerry, ibid.
[38] Kerry, ibid.
[39] Kerry, ibid.
[40] Kerry, ibid.
[41] Brian Schultz and Blade Rhoades, "Strategic Broadening for Mid-Career Cyber Leaders, paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.
[42] Schultz et al, ibid.
[43] David E. Sanger, "It's No Cold War, But Vladimir Putin Relishes His Role As Disrupter."
NY Times 30 Sep 2016; http://www.nytimes.com/2016/09/30/world/europe/for-veterans-of-the-cold-war-a-hostile-russia-feels-familiar.html
[44] David E. Sanger, "Countering Cyberattacks Without a Playbook", New York Times, 23 December 2014.
[45] Sanger, ibid.
[46] Peter Singer, "How the United States Can Win the Cyber War of the Future," *Foreign Policy,* December 8 2015.
[47] White House Policy Report, "Cyber Defense Deterrence Policy", December 2015.
[48] United States of America. The White House. Office of the President. International Strategy for Cyberspace. 16 May 2011.
[49] Department of Defense, "The DOD Cyber Strategy." op cit.
[50] BG(P) Patricia Frost, op cit.
[51] Sydney J. Freeburg, Jr. "Electronic Warfare: We Have the Technology – but Not a Strategy", Breaking Defense, 02 Dec 2015.
[52] Bryan Clark, Mark Gunzinger, "Winning the Airwaves: Regaining America's Dominance in the ElectromagnetIc Spectrum" CSBA Report, 2015.
[53] James Lewis, "Laying Down a Marker", thecipherbrief.com, October 23, 2016.
[54] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", (9 September, 2013), p. 6.
[55] Lucas Kello, "Private Sector Cyberweapons: Strategic and Other Consequences." (June 2016), Social Science Research Network.

[56] Dr Jan Kallberg, "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations" The Cyber Defense Review, Spring 2016,
[57] Schneider, ibid.
[58] Schneider, op cit.
[59] Alexander McCoy, Best Defense Guest Columnist. "We Need a Cyber Corps as a Fifth Service." Best Defense Blog, Foreign Policy Magazine, 18 March 2015.
[60] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", ibid.
[61] Lieutenant General Edward Cardon, "The Future of Army Maneuver – Dominance in the Land and Cyber Domains", The Cyber Defense Review (Spring 2016).
[62] Radhika R. Roy, Joe Law, and Rocio Bauer; TNP, CSIA, S&TCD, CERDEC, APG, MD; "Future Army Cyber Security Networking Architecture Framework", paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.
[63] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 7.
[64] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 8.
[65] Lieutenant General Edward Cardon, "The Future of Army Maneuver – Dominance in the Land and Cyber Domains," The Cyber Defense Review (Spring 2016)
[66] Zager & Zager, op cit.
[67] *The U.S. Army Landcyber White Paper, 2018-2030*, Army Cyber Command (9 September, 2013), p. 21.
[68] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit p. 13.
[69] CPT Kurtis M. Hout Jr, 1st Combat Aviation Brigade, 1st Infantry Division, Fort Riley, Kansas; "Maneuvering in an Intelligent Direction: 2 Army Cyber Dilemma's Which Need to be Addressed by the Mid-21st Century", paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.
[70] Department of Defense, "The DOD Cyber Strategy." Department of Defense, April 17, 2015.
[71] LTG Ed Cardon, Commanding General, US Army Cyber Command; "2014 Green Book: Army Cyber Command and Second Army", 30 September 2014.
[72] Sydney J. Freeburg, "Army Wargames Hone Battlefield Cyber Teams," Breaking Defense, 07 November 2016
[73] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. iii.
[74] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 16.
[75] Roy et al, op cit.
[76] LTG(R) Rhett Hernandez, Mad Scientist input, October 2016.
[77] Jamey Cummings, Comments on the Mad Scientist Panel: "Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[78] COL Carlos Vega, Army Cyber Institute; Comments on the Mad Scientist Panel:" Challenges and Opportunities in Partnerships", Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.
[79] LTC Dan Smith, Assistant Professor, USMA; Comments on the Mad Scientist Panel: "Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[80] McCoy, op cit.
[81] Andrew Tilghman, Military Times, "Does Cyber Corps Merit Its Own Service Branch?" Military Times, April 10, 2015.
[82] George M. Schwartz, Immaculata University, "Developing Cybersecurity Proficiency in an Era of Accelerating Change: Utilizing a Bachelor Degree Foundation for Emerging Professionals", paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.
[83] Dr. Marni Baker Stein, Chief Innovation Officer, University of Texas System; "Educating the Cyber Force of 2050", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[84] Schwartz, ibid.
[85] Weaver, op cit.
[86] Bruce Potter, Founder, Shmoo Group; Comments on the Mad Scientist Panel: "Community of Hackers and Makers and Innovative Thinkers", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

[87] Scott Stevenson, Comments on the Mad Scientist Panel: "Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[88] Schwartz, op cit.
[89] Schwartz, op cit.
[90] Weaver, op cit.
[91] Francesca Spidalieri and Jennifer McArdle, "Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The Role of Cybersecurity Education in US Service Academies," The Cyber Defense Review (Spring 2016).
[92] Dr. David Raymond, Deputy Director, IT Security Lab, Virginia Tech; Comments on the Mad Scientist Panel: "Educating the Cyber Force of 2050", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[93] Raymond, op cit.
[94] Margaret Andrews, "The Future of On-Campus Higher Education?" StratEDgy (blog on strategy and competition in higher education at https://www.insidehighered.com/blogs/stratedgy/future-campus-higher-education), 31 March 2015.
[95] Weaver, op cit.
[96] MG Malcolm Frost, Chief of Public Affairs, US Army; Response to Q&A at "Opening Comments / Stage Setting" Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[97] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", ibid p. 6.
[98] Scott Stevenson, op cit.
[99] Phillip Perry, "Cognitive Off-loading: How the Internet is Changing the Human Brain", Big Think, http://bigthink.com/philip-perry/cognitive-offloading-how-the-internet-is-changing-the-human-brain, 24 Aug 2016
[100] Ben FitzGerald, Peter L. Levin, and Jacqueline Parziale; "Open Source Software and the Department of Defense", Center for a New American Security (August, 2016), p. 4
[101] Fitzgerald et al, ibid p. 3
[102] Fitzgerald et al, ibid pp. 6-7.
[103] Roy et al, op cit.
[104] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 18.
[105] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 22.
[106] Roy et al, op cit.
[107] Brian David Johnson, Futurist and Fellow, Frost & Sullivan; "The Coming Age of Sentient Tools: When Our Tools are Aware, Social, and Think", Frost & Sullivan 2016.
[108] Mad Scientist Panel: "Community of Hackers and Makers and Innovative Thinkers", ibid.
[109] Roy et al, op cit.
[110] Panel Discussion, Mad Scientist Panel: "Community of Hackers and Makers and Innovative Thinkers", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016
[111] Mad Scientist Panel: "Community of Hackers and Makers and Innovative Thinkers", ibid.
[112] Hout, op cit.
[113] Dr. Jan Kallberg, "Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* (Spring 2016).
[114] Roy et al, op cit.
[115] BF(P) Frost, op cit.
[116] Joshua Toman, Chambers Clerk; Comments on the Mad Scientist Panel: "Challenges and Opportunities in Partnerships", Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.
[117] Cardon, op cit.
[118] Marene Allison and Scott Stevenson, Comments on the Mad Scientist Panel: "Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[119] Cummings, op cit.
[120] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 22.
[121] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 19.

[122] Cummings, op cit.
[123] Greg Conti, Director Information Security Research, IronNet CyberSecurity; Comments to the Mad Scientist Panel: "Community of Hackers and Makers and Innovative Thinkers", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[124] Allison, op cit.
[125] COL(R) Alex Cochran, BAE; Comments on the Mad Scientist Panel: "Who Defends the Nation in 2050?" Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.
[126] SSG Dane Sebring, Comments on the Mad Scientist Panel: "Cyber Talent Management from the Junior Perspective" Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[127] Weaver, op cit.
[128] Franklin S. Reeder and Katrina Timlin, "Recruiting and Retaining Cybersecurity Ninjas", Center for Strategic & International Studies, October 2016.
[129] SSG Anthony Quill, Comments on the Mad Scientist Panel: "Cyber Talent Management from the Junior Perspective" Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[130] Weaver, op cit.
[131] MG Frost, op cit.
[132] Weaver, op cit.
[133] CPT Rock Stevens, Comments on the Mad Scientist Panel: "Cyber Talent Management from the Junior Perspective" Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[134] Kelly Jackson Higgins, "The Kevin Durant Effect: What Skilled Cyber Security Pros Want", Information Week Dark Reading, 19 October 2016 at: http://www.darkreading.com/vulnerabilities---threats/kevin-durant-effect--what-skilled-cybersecurity-pros-want-/d/d-id/1327215
[135] Stevens, op cit.
[136] Weaver, op cit.
[137] Schneider, op cit.
[138] Kerry, op cit.
[139] Kerry, op cit.
[140] N. Turka (next note) cites "Youngstown Sheet & Tube Co. v. Sawyer" and "United States v. Curtiss-Wright Export Corp." as examples
[141] Nicholas Ryan Turza, "Counterattacking the Comment Crew: the Constitutionality of Presidential Policy Directive 20 as a Defense to Cyberattacks", North Carolina Journal of Law & Technology 15 N.C. J.L. & TECH. ON. 134 (2014).
[142] Schulz, op cit.
[143] BG(P) Frost, op cit.
[144] Cochran, op cit.
[145] Toman, op cit.
[146] Lucas Kello, "Private Cyberweapons: Strategic and Other Consequences", op cit.
[147] Toman, op cit.
[148] Weaver, op cit.
[149] Schneider, op cit.
[150] Brian David Johnson, "A Widening Attack Plain", op cit.
[151] Weaver, op cit.
[152] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. iii.
[153] Brian David Johnson, "A Widening Attack Plain", op cit.
[154] Brian David Johnson, "A Widening Attack Plain", op cit.
[155] Brian David Johnson, "A Widening Attack Plain", op cit.
[156] Brian David Johnson, "A Widening Attack Plain", op cit.
[157] Brian David Johnson, "A Widening Attack Plain", op cit.
[158] Dr Kamal Jabbour and Major Jenny Poisson, "Cyber Risk Assessment in Distributed Information Systems," *The* Cyber Defense Review (Spring 2016).

[159] Brian David Johnson, "A Widening Attack Plain", op cit.
[160] Army Cyber Command, "The U.S. Army Landcyber White Paper, 2018-2030", op cit. p. 10.
[161] Jason Healy, "The Five Futures of Cyber Conflict and Cooperation", Atlantic Council Cyber Statecraft Initiative, 2011.
[162] Jason Healy, "The Five Futures of Cyber Conflict and Cooperation", Atlantic Council Cyber Statecraft Initiative, 2011.
[163] Healy, ibid.
[164] Material section of the DOTMLPF-P Insights discussion
[165] General Panel Comments on the Mad Scientist Panel: "Who Defends the Nation in 2050?" Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.
[166] Potter, op cit.
[167] An additional panel observation: Lowest Price Technically Acceptable (LPTA) acquisition approaches mitigate against "doing things right" and lead to "just good enough to win" and the hope – not always realized – that subsequent Engineering Change Proposals (ECPs) will fix critical weaknesses.
[168] Brian David Johnson, "A Widening Attack Plain", op cit.
[169] Dr. Dave Alberts, Comments on the Mad Scientist Panel: "Challenges and Opportunities in Partnerships", Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.
[170] Stevenson, op cit.
[171] Dr Gillian Andrews, ibid.
[172] Smith, op cit.
[173] Andrew Plato, CEO of Anitian, "Building a Multi-Generational Security Program", Presentation to the Mad Scientist Conference, 14 September 2016
[174] Smith, op cit.
[175] Cochran, op cit
[176] Allison, op cit.
[177] Allison, op cit.
[178] Allison, op cit.
[179] Conti, op cit.
[180] Bill Cheswick, Visiting Scholar, University of Pennsylvania, Comments on the Mad Scientist Panel: "Community of Hackers and Makers and Innovative Thinkers", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[181] Dr Gillian Andrews, Senior XD Consultant, ThoughtWorks; Comments on the Mad Scientist Panel: "Educating the Cyber Force of 2050", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.
[182] Dr Gillian Andrews, ibid.
[183] Smith, op cit.
[184] Marene Allison
[185] Charlie Dunlap, "'Cybervandalism' or 'Digital Act of War'? America's muddled approach to cyber incidents won't deter more crises" at https://sites.duke.edu/lawfire/2016/10/30/cybervandalism-or-digital-act-of-war-americas-muddled-approach-to-cyber-incidents-wont-deter-more-crises/, 30 October 2016.

Appendix A: Workshop Design & Sources

Appendix A-1: Conference Agenda

Mad Scientist 2016:
The 2050 Cyber Army
13-14 September 2016
United States Military Academy

Agenda Day 1: 13 September 2016

0800-0850 Registration

0850-0900 Administrative Remarks, MAJ Natalie Vanatta, Army Cyber Institute

0900-0940 Welcome Remarks,
Mr. Thomas Greco, TRADOC DCS for Intelligence
LTG Robert Caslen, USMA Superintendent

0940-1015 Opening Comments / Stage Setting
MG Malcolm Frost, Chief of Public Affairs, US Army
BG (P) Patricia Frost, Director of Cyber, US Army

1015-1045 *Future Casting and the Cyber Domain*
Brian David Johnson, Futurist in Residence, Arizona State University

1045-1110 **Break**

1110-1210 *Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century*
Panel Moderator: LTC Finocchiaro, Army Cyber Institute
Jamey Cummings, KornFerry
Scott Stevenson, KornFerry
Marene Allison, CISO, Johnson & Johnson
LTC Dan Smith, Assistant Professor, United States Military Academy

1210-1400 **Lunch Break**

1315-1400 *Tour of Branch Displays (Meet at Patton's Statue)*

APPENDIX A: WORKSHOP DESIGN & SOURCES
A-1: CONFERENCE AGENDA

1400-1500 *Educating the Cyber Force of 2050*
Panel Moderator: LTC Clay Moody, ECCS
Dr. David Raymond, Deputy Director, IT Security Lab, Virginia Tech
Dr. Marni Baker Stein, Chief Innovation Officer, University of Texas System
Dr. Gillian "Gus" Andrews, Senior XD Consultant, ThoughtWorks

1500-1600 *Community of Hackers and Makers and Innovative Thinkers*
Panel Moderator: CPT Brent Chapman, DiUX
Greg Conti, Director Information Security Research, IronNet CyberSecurity
Bruce Potter, Founder, Shmoo Group
Bill Cheswick, Visiting Scholar, University of Pennsylvania

1600-1620 **Break**

1620-1720 *Cyber Talent Management from the Junior Perspective*
Panel Moderator: MAJ Brian Schultz, ACI
CPT Rock Stevens
CPT Josh Lospinoso
SSG Dane Sebring
SSG Andrew Quill

1720-1730 Closing Remarks
Mr. Thomas Greco, TRADOC DCS for Intelligence

1800-2000 No-Host Social

Agenda Day 2: 14 September 2016

0810-0830 Welcome Remarks
MAJ Natalie Vanatta, Army Cyber Institute

0830-0915 *Building a Multi-Generational Security Program*
Andrew Plato, CEO of Anitian

0915-1015 *Challenges and Opportunities in Partnerships*
Panel Moderator: COL Carlos Vega, Army Cyber Institute
F. Edward Goetz, VP and CSO, Exelon Corporation
Bill Hutchinson, CEO SIMSPACE
Joshua Toman, Chambers Clerk

APPENDIX A: WORKSHOP DESIGN & SOURCES
A-1: CONFERENCE AGENDA

1015-1045 **Break**

1045-1130 *Unconventional Teams and the Power of Seeing the Invisible*
Gayle Lemmon, Author of *Ashley's War* and *The Dressmaker*

1130-1215 *Pervasive Capability: Our Only Hope*
Matthew Weaver, Rogue Leader, Defense Digital Service

1215-1345 **Lunch Break**

1345-1445 *Who Defends the Nation in 2050?*
Panel Moderator: MAJ Joshua Bundt, Army Cyber Institute
David Tohn, CEO BTS-S2
Alex Cochran, BAE
COL James Raftery, Deputy Head EECS, United States Military Academy

1445-1515 *Partnerships: Today and Tomorrow*
COL Andrew Hall, Director of the Army Cyber Institute

1515-1540 **Break**

1540-1625 *Ladyada – Entrepreneur, Hacker, Maker, Artist, and Engineer – Adafruit Factory*
Limor Fried, CEO of Adafruit

1625-UTC Closing Remarks
COL Andrew Hall, Director of the Army Cyber Institute

Appendix A-2: Conference Presenters

(IN ALPHABETICAL ORDER BY LAST NAME)

Marene Allison, ***President and Chief Information Security Officer, Johnson & Johnson*** *(Day 1 Panel)*

Dr. Gillian "Gus" Andrews, ***Senior XD Consultant, ThoughtWorks*** (Day 1 Panel)

Dr. Marni Baker ***Chief Innovation Officer, University of Texas System's Institute for Transformational Learning,*** (Day 1 Panel)

MAJ Josh Bundt ***Cyber Education Instructor, Army Cyber Institute*** (Day 2 Panel)

LTG Robert Caslen, Jr., ***59th Superintendent, United States Military Academy*** (Day 1 Welcoming Remarks)

CPT Brent Chapman, ***Instructor, Department of Electrical Engineering & Computer Science, United States Military Academy*** (Day 1 Panel)

Mr. Bill Cheswick, ***Visiting Scholar, University of Pennsylvania, Co-Founder, Lumeta Corp.*** (Day 1 Panel)

Mr. Gregory Conti, ***Director of Information Security Research, IronNet Cybersecurity*** (Day 1 Panel)

Mr. Jamey Cummings, ***Senior Partner, KornFerry Global Technology Practice*** (Day 1 panel)

LTC James Finocchiaro, ***Research Scientist, Army Cyber Institute*** (Day 1 Panel)

Ms. Limor Fried, ***Founder, Adafruit Industries*** (Day 2)

MG Malcolm Frost, ***Chief of Public Affairs, United States Army*** (Day 1 Opening Comments)

BG (P) Patricia Frost, ***Deputy Commander for Operations, United States Army Cyber Command and Second Army*** (Day 1 Opening Comments)

Mr. F. Edward Goetz, ***Vice President and Chief Security Officer, Exelon***

Corporation (Day 2 Panel)

Mr. Thomas Greco, *Deputy Chief of Staff, G-2, United States Army Training and Doctrine Command* (Day 1 Opening and Closing Remarks)

COL Andrew Hall, *Director, Army Cyber Institute* (Day 2 and Day 2 Closing Remarks)

Mr. Bill Hutchinson, *CEO, Co-Founder, SIMSPACE* (Day 2 Panel)

Mr. Brian David Johnson, *Arizona State University, Center for Science and the Imagination, Frost & Sullivan* (Day 1)

Ms. Gayle Lemmon, *Author* (Day 2)

CPT Josh Lospinoso, *United States Army* (Day 1 Panel)

LTC Clay Moody, *Assistant Professor, United States Military Academy* (Day 1 Panel)

Mr. Andrew Plato, *CEO, Anitian* (Day 2)

Mr. Bruce Potter, *Chief Technology Officer, KEYW Corporation, Founder, Shmoo Group* (Day 1 Panel)

SSG Andrew Quill, *United States Army* (Day 1 Panel)

COL James Raftery, *Associate Professor and Deputy Head, United States Military Academy* (Day Two Panel)

Dr. David Raymond, *Director, Virginia Cyber Range, Deputy Director, IT Security Lab, Adjunct Associate Professor, Bradley Department of Electrical and Computer Engineering, Virginia Tech* (Day 1 Panel)

MAJ Brian Schultz, *Army Cyber Institute* (Day 1 Panel)

LTC Dan Smith, *Assistant Professor of Behavioral Science and Leadership, United States Military Academy, Senior Editor, West Point Leadership* (Day 1 Panel)

SSG Dane Sebring, *United States Army* (Day 1 Panel)

CPT Rock Stevens, *United States Army* (Day 1 Panel)

Mr. Scott Stevenson, *KornFerry Global Technology Practice* (Day 1 Panel)

Mr. Josh Toman, *Chambers Clerk to the Honorable Frank D. Whitney* (Day 2 Panel)

MAJ Natalie Vanatta, *Army Cyber Institute* (Day 1 Administrative Remarks, Day 2 Welcoming Remarks)

COL J Carlos Vega, *Instructor, Director of Outreach, Army Cyber Institute* (Day 2 Panel)

Mr. Matthew Weaver, *Rogue Leader, Defense Digital Service* (Day 2)

Appendix A-3: Conference Presentations

(IN ORDER OF PRESENTATION)

DAY ONE, 13 September 2016

Welcome Remarks
Mr. Thomas Greco, *U.S. Army TRADOC DCS for Intelligence*
LTG Robert Caslen, *United States Military Academy Superintendent*

Telling The Army Story: Engaging the American People
MG Malcolm Frost, *Chief of Public Affairs, US Army*

Cyberspace Operations/SIGINT/EW Integration Update
BG (P) Patricia Frost, *Director of Cyber, US Army*

A Widening Attack Plain: Initial Cyber Threatcasting Report out for Mad Scientist
Brian David Johnson, *Futurist in Residence, Arizona State University*

Panel: Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century [No Briefing]
Panel Moderator: LTC Finocchiaro, *Army Cyber Institute*
Jamey Cummings, *KornFerry*
Scott Stevenson, *KornFerry*
Marene Allison, *CISO, Johnson & Johnson*
LTC Dan Smith, *Assistant Professor, USMA*

Panel: Educating the Cyber Force of 2050 [No Briefing]
Panel Moderator: LTC Clay Moody, *ECCS*
Dr. David Raymond, Deputy Director, *IT Security Lab, Virginia Tech*
Dr. Marni Baker Stein, *Chief Innovation Officer, University of Texas System*
Dr. Gillian "Gus" Andrews, *Senior XD Consultant, ThoughtWorks'*

Panel: Community of Hackers and Makers and Innovative Thinkers [No Briefing]
Panel Moderator: CPT Brent Chapman, *DiUX*
Greg Conti, *Director Information Security Research, IronNet CyberSecurity*
Bruce Potter, *Founder, Shmoo Group*
Bill Cheswick, *Visiting Scholar, University of Pennsylvania*

Panel: Cyber Talent Management from the Junior Perspective [No Briefing]

Panel Moderator: MAJ Brian Schultz, *ACI*
CPT Rock Stevens
CPT Josh Lospinoso
SSG Dane Sebring
SSG Andrew Quill

Concluding Remarks [No Briefing]
Mr. Thomas Greco, *U.S. Army TRADOC DCS for Intelligence*

DAY TWO, 14 September 2016

Building a Multi-Generational Security Program
Andrew Plato, *CEO of Anitian*

Challenges and Opportunities in Partnerships [No Briefing]
Panel Moderator: *COL Carlos Vega, Army Cyber Institute*
F. Edward Goetz, *VP and CSO, Exelon Corporation*
Bill Hutchinson, *CEO SIMSPACE*
Joshua Toman, *Chambers Clerk*

Unconventional Teams and the Power of Seeing the Invisible
Gayle Lemmon, Author of *Ashley's War* and *The Dressmaker*

Pervasive Capability: Our Only Hope
Matthew Weaver, *Rogue Leader, Defense Digital Service*

Who Defends the Nation in 2050? [No Briefing]
Panel Moderator: MAJ Joshua Bundt, *Army Cyber Institute*
David Tohn, *CEO BTS-S2*
Alex Cochran, *BAE*
COL James Raftery, *Deputy Head EECS, USMA*

Partnerships and the Cyber Domain
COL Andrew Hall, Director of the Army Cyber Institute

Ladyada – Entrepreneur, Hacker, Maker, Artist, and Engineer – Adafruit Factory [No Briefing]
Limor Fried, *CEO of Adafruit*

Closing Comments [No Briefing]
COL Andrew Hall, *Director of the Army Cyber Institute*

Appendix A-4: Submitted Papers

(IN LEAD AUTHOR ALPHABETICAL ORDER)

"Maneuvering in an Intelligent Direction: 2 Army Cyber Dilemmas Which Need to be Addressed by the Mid-21st Century." CPT Kurtis Hout

> The U.S. Army's Cyber proliferation initiatives in the development, advancement, and ultimately weaponization of the cyber domain has arguably been one of our Army's highest priorities as of late. Cyber is now not only an Army branch, but the profession has also massaged itself into the discussion of arenas such as Intelligence, Signal, and Space Operations. However, the Army's push for cyber to become a focal point of the battlefield does have missing nuances that must be addressed by the mid twentieth century if we are to remain as the premier ground force, that fights and wins our Nation's wars. First, policy makers must accept the reality that the cyber domain includes EMP threats. Second, the Army must refine its view of warfighting functions given the dynamics of the cyber domain to ensure that it can properly train and equip solders to operate in the domain.

"Future Army Cyber Security Networking Architecture Framework." Radhika R. Roy, Joe Law, and Rocio Bauer

> Zero-day-vulnerabilities that remain in software, firmware, and hardware unknown to their developers which are exploited by cyber criminals are the fundamental cause of attacks. This paper proposes a cyber security architecture that will enable detect, isolate, and repair after cyber-attacks for both known and unknown attacks of the communications functional elements using end-to-end secure call tracing and immunization algorithms on runt-time dynamically for both data payload and control signaling traffic.

"Training Future Cyber Officers." Cadet Andrew Schoka

> The importance of properly preparing and developing the leaders of the Army cyber force is an issue that requires the continued attention of Army leaders in

order to ensure the long-term viability of the Army's warfighting efforts in the cyber domain. This paper provides an analysis of the current developmental framework used by the Army ROTC to train, develop, and select its future cyber officers, and propose specific, actionable steps to be taken in order to address the current lack of a formalized system for performing this critical function.

"Strategic Broadening for Mid-Career Cyber Leader." Brian Schultz and Blake Rhoades

Proficiency in cyberspace tactics can create a base of knowledge for leaders to understand the domain, but the Army must sow the seeds of strategic and policy education in cyberspace leaders as they approach mid-career. This paper highlights the need for strategic broadening and policy education for mid-career cyberspace leaders, while also providing an overview of available broadening programs that have a short-term, in-person format. As any leader progresses through the ranks, the Army often requires different skills at higher levels of responsibility; cyberspace will not be an exception. The two programs described in this paper provide a view in developing mid-career leaders in the realm of strategy and policy related to cyberspace and outlines these how these programs might be structured in terms of eligibility, coursework, and outcomes.

"Developing Cybersecurity Proficiency in an Era of Accelerating Change: Utilizing a Bachelor Degree Foundation for Emerging Professionals." George Schwartz, George M**.**

This paper addresses the key question: What is the best way to develop cybersecurity professionals to reduce the gap between the demand and supply, and what is the role of higher education in helping to meet future needs? This paper advocates a cyber training regimen that allows graduates to:
graduates to be able to:

- Effectively lead efforts to improve its cybersecurity in an organization through collaboration and change management.
- Conduct cybersecurity research and prepare recommendations that can be used to enhance an organization's security standards against threats.
- Apply ethical decision-making models to cybersecurity challenges.
- Monitor information technology (IT) security trends regarding threats and

critically assess current information assurance practices and countermeasures.
- Recognize the global threats to cyber networks, and assess the risks associated with an organization's systems.
- Design broad and holistic security solutions, recommend required changes for their organization, and manage the implementation of security systems including policies and procedures.

"Why We Will Continue to Lose The Cyber War." Robert Zager and John Zager

The first wave of cyber security was focused on perimeter controls with tools such as firewalls, gateways and anti-virus protection. The second wave of security brought Security Information Event Management ("SIEM") to bear. The volume of SEIM information which must be processed is driving the third wave of cyber security, termed "cyber threat intelligence," in which analytic tools are used to observe data in real time and report deviations from known patterns. IBM is now promoting the next wave of cyber security, which it dubs "cognitive security. This paper, argues that cyberintelligence solutions, such as cognitive security and cyber threat intelligence, are fundamentally flawed approaches that cannot deliver what they promise. Cyberintelligence is an important, but insufficient, approach to cybersecurity. Cyberintelligence must be subsumed into the larger "Methodology for Adversary Obstruction."

Appendix A-5: Survey Contributors

(COMPLETE ENTRIES IN ALPHABETICAL ORDER BY LAST NAME)

1. **Paul Bresnowitz, U.S. Army ARDEC**
2. **Helena Keeley, Compsim**
3. **Alexander Hubert, HQDA G-4 LIA**
4. **Morgan Rockwell Bitcoin, Inc.**
5. **Radhika Roy, CSIA CERDEC**
6. **John Zager, PepsiCo**
7. **Kira Hutchinson, TRADOC G-2**
8. **George Schwartz, Immaculata University**
9. **Earnest Moore, ARDEC**
10. **Ernesto Lopez, ARDEC**
11. **Robert Zager, Iconix**
12. **Kurtis Hout, U.S. Army**
13. **Steffany Trofino, N/A (USG)**

Appendix B: Army Warfighting Challenge and Technology Imperative Insights

Appendix B-1: Army Warfighting Challenge Insights

This section of the study aligns each of the key observations and insights developed during and after the Mad Scientist: 2050 Cyber Army Conference with each of the 20 Army Warfighting Challenges. Each observation is tagged by the Quicklook Report framework element (*Challenge of Cyber*, *Strategic Context*, or *DOTMLPF-P Insights, Cyber Futures, or Cyber Change Management*) followed by the relevant report subheading.

Army Warfighting Challenges are enduring first-order problems, the solutions to which improve the combat effectiveness of the current and future force. Aligning the observations and insights in this way is intended to assist in the Army in developing solutions to each over the course of the overall campaign of learning.

1. Develop Situational Understanding

How to develop and sustain a high degree of situational understanding while operating in complex environments against determined, adaptive enemy organizations.

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/Domain Dilemmas:* Cyber effects can have global reach and effortlessly cross legacy geographic boundaries.
- *Challenge of Cyber/Domain Dilemmas:* Ambiguity makes cyber effects more – rather than less – relevant for adversaries in pursuit of “gray zone” strategies.
- *Challenge of Cyber/Domain Dilemmas:* Cyber effects are the principal bridge between the physical and cognitive dimensions of conflict, and – through information warfare – impact the moral domain (the domain of belief).
- *Challenge of Cyber/Planning:* Many cyber intelligence tools are forensic in nature.
- *Challenge of Cyber/Cyber-Casting:* The rate of change in cyber science frustrates forecasting. The unique characteristics of the cyber domain frustrate the predictive power we expect in military theories and strategy. Battle results are indirect, not readily observable and difficult to quantify. Actors are anonymous, and engagements happen at machine speed.

- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* What does "doctrine" mean when the highest form of cyber art is the unprecedented, "zero-day" attack?
- *Strategic Context/Interests in Cyberspace:* Because of the ubiquity of the impacts of digitization, our interests in cyberspace are generally congruent to national interests, but with influences (and impacts) that are more global because of the global interconnectivity of cyber infrastructure. There is little indication that these interests will substantively change out to 2050
- *Strategic Context/Economy Linkages:* With a strong American economy recognized as the "foundation of U.S. power," increasingly the digital economy is a vital element of this strength.
- *Strategic Context/Economy Linkages:* Digitization, like electricity, is a general-purpose technology that underpins a huge share of economic activity beyond the sector that supplies it.
- *Strategic Context/Economy Linkages:* The digital economy is growing rapidly, and in the United States and around the globe is more resilient and faster-growing than the economy as a whole.
- *Strategic Context/Economy Linkages:* The digital / cyber economy presents significant challenges to economic equality and the future of work.
- *Strategic Context/Economy Linkages:* Most nation-states are adopting strategies aimed at improving their digital competitiveness by expanding infrastructure, developing e-government, and directly promoting digital industries.
- *Strategic Context/Deterrence:* Cyber attackers are hard to identify with certainty, and the evidence cannot be made public.
- *Strategic Context/Deterrence:* Deterrence is hard to establish. Because there are no international treaties or norms about the use of digital weapons by states, non-state groups or individuals – or even acknowledgment by the U.S. Government that it has ever used them itself -- there are effectively no rules to constrain cyber conflict.
- *Strategic Context/Cyber Strategies:* The DOD cyber strategy focuses on building cyber capabilities and organizations for DoD's three primary cyber missions: to defend DoD networks, systems, and information; defend the Nation against cyberattacks of significant consequence; and provide cyber support to operational and contingency plans. Its sets five strategic goals for cyber forces to achieve.
- *Strategic Context/Cyber Power:* The most capable and least risky future military is one in which digital technologies enhance capabilities but are not uniquely critical vulnerabilities.
- *DOTMLPF-P Insights/Doctrine:* Doctrine typically draws from theory, but with respect to theory, any future cyber doctrine confronts several challenges, including no dominant theory to describe cyber's bridge between the physical,

cognitive, and moral dimensions of conflict; physical metaphors that do not match the cyber domain, and the growth of capabilities that far outpaces relevant theory and doctrine.

- *DOTMLPF-P Insights/Organization:* Now that cyber is a domain, proposals for a Cyber Service will be inevitable.
- *DOTMLPF-P Insights/Material:* Internet of things, centralization and decentralization, connectivity, and smart grid arrays will define cyber technology developments.
- *DOTMLPF-P Insights/Material:* Sentient Tools are "what comes next" and emerge from a base of computational, sensing and communications technologies that have been advancing for over the last 50 years. Sentient Tools will drive the next phase of development of computational systems, smart cities and environments, autonomous systems, artificial intelligence, big data and data mining, and an interconnected system in the Internet of Things (IoT).
- *DOTMLPF-P Insights/Material:* Many of our current security vulnerabilities are by design; over time many of these design flaws can be corrected. Several disruptive materiel solutions may mitigate some cyber vulnerabilities, including for example quantum sensing and quantum communication, read-Only Memory (ROM), and security models that mimic biological systems
- *DOTMLPF-P Insights/Facilities:* The centralization trend of some cyber technologies such as cloud computing positions those central facilities as significant targets for either cyber or kinetic attack.
- *DOTMLPF-P Insights/Facilities:* The cyber domain is itself an infrastructure of capabilities and vulnerabilities that connects to a family of weapons and platforms. In that sense, the advancements that cyber technologies bring to modern conflict may be better likened to the impact of the development of roads, railroads, or combustion engines than to the rifle, the tank, or the aircraft carrier.
- *DOTMLPF-P Insights/Facilities:* Although cyber actions can occur at machine speed and the technology can advance very rapidly, some aspects of the cyber domain infrastructure such as cell tower systems, fiber-optic cable or satellite constellations require years if not decades of anticipation, planning and investment.
- *DOTMLPF-P Insights/Policy:* The consequences and visibility of key cyber issues like data privacy and security, surveillance, and internet management have grown and are addressed at levels far above the Army; in many cases: by the President. Those policies nonetheless directly impact Army preparation for and execution of cyber operations.
- *DOTMLPF-P Insights/Policy:* Some issues of cyber policy will migrate to the level of constitutional issues.

- *DOTMLPF-P Insights/Policy:* Some of our most important future cyber capabilities, such as digital resiliency, will not be possible without an effective policy foundation.
- *DOTMLPF-P Insights/Policy:* The Law of Cyber Warfare is not established. For instance, the North Atlantic Treaty expressly states the right to collective defense in the face of "armed conflict" but lacks language accounting for cyber warfare.
- *DOTMLPF-P Insights/Policy:* Because cyber infrastructure is simultaneously a delivery mechanism for both the economic and social benefits of information and communication technology, as well as weaponized cyber threats, bridging the "internet-cyber" gap is a conundrum for policy makers and will limit the optimization of policy for Army and Joint operations.
- *Cyber Futures/Alternative Cyber Futures:* Possible future cyber worlds include: Status Quo, Conflict Domain, Balkanization, Paradise, and Cybergeddon.
- *Cyber Change Management/Vision:* Future cyber vision must account for inevitable ubiquity and pervasiveness of cyberspace. It must feature *unity of cyberspace*: for the battlefield of 2050 the appropriate relationships, doctrine and arrangements and concepts must be built jointly between industry, militaries of different countries, and inter agency partners.
- *Cyber Change Management/Risk Management:* Most of cyber-security is risk management. You have to broaden the scope to integrate cultural and process solutions with technical solutions.
- *Cyber Change Management/Risk Management:* There is a tension in the cyber industry between the desire for speed to market and security.

2. Shape the Security Environment

How to shape and influence security environments, engage key actors, and consolidate gains to achieve sustainable security outcomes in support of Geographic and Functional Combatant Commands and Joint requirements.

<u>Mad Scientist: 2050 Cyber Army Related Observations</u>

- *Challenge of Cyber/Planning:* For the United States, reaction (and defense) is decentralized; action (and offense) tends to be highly centralized. The offense / defense dynamic is also symmetric to our adversaries, who frequently decentralize their offensive operations.
- *Challenge of Cyber/Categorization Conundrum:* Cyber – and the digitization that underlies it – is ubiquitous and impacts everything. This ubiquity confounds our traditional approaches to categorization in almost every field, with a "boundary busting" impact that diffuses the distinctions between civil and military action,

between the physical / informational / moral dimensions of conflict, and across the diplomatic, informational, military, and economic (DIME) elements of power.

- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* How do we plan for cyber infrastructure considerations that are global and external to military control?
- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* How will the Army shape governing policy that typically originates and is decided outside of its decision purview?
- *Strategic Context/Deterrence:* Deterrence options may include sanctions, indictments, cyber retaliatory options, and even the threat of kinetic measures. The ubiquity of cyberspace weapons and the difficulty of attribution in cyberspace means that our traditional deterrence options will not always succeed against a variety of cyber threats.
- *Strategic Context/Deterrence:* Cyber deterrence will be centered on "deterrence by denial" — making attacks less probable by reducing their likely value through cyber resilience.
- *Cyber Futures/Alternative Cyber Futures:* The key discriminator for the outcome of Alternative Cyber Futures is the outcome of the cyber contest between offensive and defensive cyber operations.
- *Cyber Futures/Risky Assumptions:* That this threat is not existential. We don't see cyber as an existential threat but for many industries it is exactly that; intellectual property theft happens every day, and for many individuals, the majority of their "existence" is within the cyber domain.
- *Cyber Futures/Risky Assumptions:* That large nation-state competitors would never resort to cyber warfare because they are too inter-dependent with us.

3. Provide Security Force Assistance

How to provide security force assistance to support policy goals and increase local, regional, and host nation security force capability, capacity, and effectiveness.

<u>Mad Scientist: 2050 Cyber Army Related Observations</u>

- *Strategic Context/Cyber Power:* The cyber domain exhibits a sovereignty gap: the Government cannot protect the private sector against all relevant threats. The challenge of cybersecurity, therefore, is essentially one of civil defense: how to equip the private sector to protect its own computer systems in the absence of decisive government involvement.

4. Adapt the Institutional Army

How to maintain an agile institutional Army that ensures combat effectiveness of the total force, supports other services, fulfills DoD and other agencies' requirements, ensures quality of life for Soldiers and families, and possesses the capability to surge (mobilize) or expand (strategic reserve) the active Army.

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* Can an industrial age acquisition system accommodate "material" concerns where the most relevant "system" is typically at the sub-platform level and the most significant part of that system is "software" vice "hardware," and "open-sourced" is considered more effective than "closed-sourced?
- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* Can our legacy personnel policies deal with technology impacts that include significant alteration of our very thinking processes?
- *Strategic Context/Cyber Strategies:* The Army Cyberspace Strategy for Unified Land Operations in 2025 seeks to integrate cyber forces, capabilities, facilities, and partnerships to execute Joint and Army operations and to support the DoD strategy along five Lines of Effort: LoE 1: Build the Workforce; LoE 2: (Offensive / Defensive) Operations; LoE 3: Capability Development; LoE 4: Facilities, Systems and Infrastructure; LoE 5: Partnerships.
- *Strategic Context/Cyber Strategies:* The Army Cyber Center of Excellence Strategy pursues a vision of a highly-skilled workforce that effectively collaborates with relevant stakeholders to develop and lead integrated cyber, signal, and electronic warfare and signal solutions (capabilities) for the Army and Joint Forces.
- *DOTMLPF-P Insights/Organization:* The convergence of time and space, technology and functional synergy increasingly will compel the Army to find ways to seamlessly integrate and unify the operational and institutional force, enabling operational force reach back to the institutional force to solve fast-paced emerging problem sets.
- *DOTMLPF-P Insights/Organization:* The Reserve component will use existing forces to augment Army requirements for operating in the cyberspace domain.
- *DOTMLPF-P Insights/Material:* Open Source software development models are generally better than their proprietary counterparts because they can take advantage of the brainpower of larger teams, which leads to faster innovation, higher quality, and superior security for a fraction of the cost.

- *DOTMLPF-P Insights/Leadership and Education:* There will be a war for talent, particularly cyber leaders, across our society. The Army must think now about how to motivate and retain its most effective cyber leaders.
- *DOTMLPF-P Insights/Policy:* Automated cyber engagements may require rethinking legacy Title 10 and Title 50 boundaries.
- *Cyber Futures/Risky Assumptions:* That we must allocate a lot of time and energy determining each Service's role in the cyber domain. Allocation of roles (based on legacy boundaries) takes us down a path that is not tenable.
- *Cyber Futures/Risky Assumptions:* That it's OK to accept software that we know is fundamentally inadequate.
- *Cyber Change Management/Culture:* Culture is a key foundation for effective change.
- *Cyber Change Management/Culture:* The risk culture within Government agencies must shift mentality from "check the box" compliance to more active risk management.
- *Cyber Change Management/Culture:* Change management must account for default cultures associated with distinct societal "generations.
- *Cyber Change Management/Risk Management:* Lowest Price Technically Acceptable (LPTA) acquisition approach mitigates against "doing things right" and leads to "just good enough to win" and the hope – not always realized – that subsequent Engineering Change Proposals (ECPs) will fix critical weaknesses.

5. Counter Weapons of Mass Destruction

How to prevent, reduce, eliminate, and mitigate the use and effects of weapons of mass destruction (WMD) and chemical, biological, radiological, nuclear, and high yield explosives (CBRNE) threats and hazards on friendly forces and civilian populations.

Mad Scientist: 2050 Cyber Army Related Observations

- No observations recorded during the Mad Scientist: 2050 Cyber Army Conference related to this Army Warfighting Challenge.

6. Conduct Homeland Operations

How to conduct homeland operations to defend the Nation against emerging threats.

Mad Scientist: 2050 Cyber Army Related Observations

- *DOTMLPF-P Insights/Organization:* Because of the cross-boundary ubiquity and reach of cyber operations, organizational solutions are problematic.

- *DOTMLPF-P Insights/Policy:* The issue of enabling "civil defense" in the cyber domain is problematic, with some positing the possibility of "letters of marque," or "cyber Blackwater" and others warning of dire consequences if authority for pre-emptive or counter-offensive action is delegated to the civilian sector.

7. Conduct Space and Cyber Electromagnetic Operations and Maintain Communications

How to assure uninterrupted access to critical communications and information links (satellite communications [SATCOM], positioning, navigation, and timing [PNT], and intelligence, surveillance, and reconnaissance [ISR]) across a multi-domain architecture when operating in a contested, congested, and competitive operating environment.

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/Planning:* The greater the reliance on advanced cyber capabilities – both as direct weapons and as enablers for conventional capabilities – the greater the potential disruption, diversion, and destruction that adversaries can create via malicious cyber activities in the future.
- *Strategic Context/Cyber Strategies:* The Electronic Warfare function lacks a coherent vision and strategy at both DoD and Army levels.
- *Strategic Context/Cyber Power:* To practice effective mission command, sustain the forces, provide critical intelligence, and communicate over the horizon, a nation must be a cyber and space power.
- *DOTMLPF-P Insights/Doctrine:* Doctrinal "levels of war" of war pose unique challenges in the cyber domain, with tactical actions having global reach, and significant "sub-platform warfare" that can be isolated to singular platforms or pervasive, damaging lower layer infrastructure like Operating Systems (OSs), BIOS, hardware, hard drives, and memory disks, and thereby crippling widespread capabilities and services that depend on these lower layers.
- *DOTMLPF-P Insights/Material:* Electromagnetic Pulse (EMP) Vulnerabilities. Near-peer competitors like Russia, China, North Korea, and Iran all make EMP attack a complementary part of their cyber doctrine.

8. Enhance Training

How to train Soldiers and leaders to ensure they are prepared to accomplish the mission across the range of military operations while operating in complex environments against determined, adaptive enemy organizations.

APPENDIX B: ARMY WARFIGHTING CHALLENGE & TECHNOLOGY CHALLENGE INSIGHTS
B-1: ARMY WARFIGHTING CHALLENGE INSIGHTS

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* How will any training system address the fact that cyber technologies will advance several cycles over the duration of a typical military career?
- *DOTMLPF-P Insights/Training:* Future training can leverage simulation or gaming technology aided by artificial intelligence that replicates real terrain, physical structures, and social interaction in cyberspace.
- *DOTMLPF-P Insights/Training:* Cyber capabilities must be incorporated into exercises in order to establish credibility with the broader operational force.
- *DOTMLPF-P Insights/Training:* Cyber technologies are accelerating the process of 'cognitive off-loading' in humans, whereby computational / cognitive tools shorten our attention spans and memory, impacting education and learning.
- *DOTMLPF-P Insights/Training:* For legacy DOTMLPF-P analysis, education is associated with leader development; in the cyber domain education will be inseparable from training and certification.
- *DOTMLPF-P Insights/Training:* Cyber warriors are "knowledge workers," as such they need more than "training," they need a strong education in cyber fundamentals in order to enable an understanding of the complexity of the cyber domain.
- *DOTMLPF-P Insights/Training:* Such an education, however, is not enough. They also require technical certifications in such areas as cybersecurity tools, information security, and network engineering.
- *DOTMLPF-P Insights/Training:* Although certifications are emerging as one of the most important dimensions of cyber training, accelerating changes in technology could make current certifications obsolescent. The solution will be a life-long approach to learning (and certification) in the cyber domain. As cyber technology becomes ubiquitous, so too must a fundamental set of cyber skills. These skills can no longer be relegated to IT organizations.
- *DOTMLPF-P Insights/Training:* Cyber education must be multi-disciplinary must extend outside of the classroom environment.
- *DOTMLPF-P Insights/Training:* Cybersecurity is a complex subject, whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law.
- *DOTMLPF-P Insights/Training:* Essential cybersecurity job requirements include soft (non-technical) skills, specifically: leadership, communications ability, and interpersonal skills. Thus while higher education may not be able to keep up with rapidly changing technology, it can provide a solid foundation for emerging cybersecurity professionals.

- *DOTMLPF-P Insights/Training:* The lifespan of a technical cyber degree is three years. Because of the rate of technical change, cyber training and education must be self-directed, modular, open-loop, and lifelong.
- *DOTMLPF-P Insights/Training:* The key skills required are: problem solving / influencing / relationship-building.
- *DOTMLPF-P Insights/Leadership and Education:* Future cyber leader education must broaden their abilities to conceptualize rapidly and develop creative feasible solutions to complex challenges. They must be able to succinctly convey succinctly complicated cyberspace conceptual or analytical material in a manner that is understood clearly by decision-makers.
- *DOTMLPF-P Insights/Leadership and Education:* Conflicts in cyberspace will also require a profound understanding of foreign culture, foreign languages, and intelligence capabilities, use of diplomatic means, Army foreign area operations, IIA, cyberspace operations, and civil affairs operations.
- *DOTMLPF-P Insights/Policy:* Authorities have the negative impact of keeping commanders from not training on things they are not authorized to do.
- *Cyber Change Management/Culture:* Our institutions cannot educate for creative, flexible thinking without significant cultural change.
- *Cyber Change Management/Culture:* You cannot change culture without changing process, including the very process of education. Pedagogy does not work does not work for technology innovation: students must build knowledge out of an ecology of ideas.

9. Improve Soldier, Leader and Team Performance

How to develop resilient Soldiers, adaptive leaders, and cohesive teams committed to the Army professional ethic that are capable of accomplishing the mission in environments of uncertainty and persistent danger.

<u>Mad Scientist: 2050 Cyber Army Related Observations</u>

- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* What is the role of leaders (and their education) when they will rarely be the most technically competent (or experienced) member of their organization?
- *DOTMLPF-P Insights/Organization:* Organizational solutions in the cyber domain will typically include extensive use of inter-disciplinary teaming and partnering, putting a premium on cross-institutional transparency, trust building, and collaboration.
- *DOTMLPF-P Insights/Personnel:* People are typically the "weak link" in cyber engagements, in fact, insider threats typically do more damage to cyber capabilities (and to institutions) than external adversaries.

- *DOTMLPF-P Insights/Personnel:* For the Army of 2050, as cyber becomes ever more entwined with the fabric of our systems and our institutions, every Soldier will be a Cyber Warrior.
- *DOTMLPF-P Insights/Personnel:* The fundamentals for Cyber Warriors include passion, critical thinking, and problem-solving.
- *DOTMLPF-P Insights/Personnel:* Money will not be as useful for retention of future cyber talent as empowerment.
- *DOTMLPF-P Insights/Personnel:* The future may present fundamentally altered career models wherein cyber professionals routinely transfer between DoD and private industry. There could be a revolving door that works in both directions.
- *DOTMLPF-P Insights/Personnel:* Many individuals are in the cyber components of the military because of patriotism, an interesting problem space, and the desire to make an impact. A sense of purpose is the greatest recruiting tool.
- *DOTMLPF-P Insights/Personnel:* One of the best ways to enhance cyber recruiting would be to lower the barrier of understanding between the US population and their government / military.
- *DOTMLPF-P Insights/Personnel:* The Army (and Navy) direct commissions for dentists and doctors, why not for cyber talent?
- *DOTMLPF-P Insights/Personnel:* To get ready for 2050, the Army needs to stop recruiting at shopping malls. Recruit at STEM programs; find cyber aptitude in middle and high school and develop relationships that support and encourage youth to serve in the Army.
- *Cyber Change Management/Culture:* There is an important role for meta-cognition: the ability to recognize the ideas we already hold.
- *Cyber Change Management/Culture:* A culture of innovation within the cyber community requires thinkers who are willing to give more than they take, step outside the box, bridge communities, and build relationships.
- *Cyber Change Management/Ownership:* A sense of ownership is essential to effective cyber change management, but if future cyber is ubiquitous and pervasive, who will “own it?”
- *Cyber Change Management/Ownership:* “Stop thinking of who is in and who is out in fighting cyber war. We’re all in.”

10. Develop Agile and Adaptive Leaders

How to develop agile, adaptive, and innovative leaders who thrive in conditions of uncertainty and chaos and are capable of visualizing, describing, directing, and leading and assessing operations in complex environments and against adaptive enemies.

APPENDIX B: ARMY WARFIGHTING CHALLENGE & TECHNOLOGY CHALLENGE INSIGHTS
B-1: ARMY WARFIGHTING CHALLENGE INSIGHTS

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/Cyber-Casting:* Cyber forecasting and cyber threat-casting is a framework for understanding (not prediction). Forecasts must be multidisciplinary, incorporate "gates" to alert us to decision points where we can shape the desired future, and "flags" to confirm or deny our forecasts.
- *DOTMLPF-P Insights/Doctrine:* Commanders will recognize the principles of maneuver warfare as equally applicable in cyberspace: targeting critical vulnerabilities; audacity; surprise; focus; decentralized decision-making; tempo.
- *DOTMLPF-P Insights/Doctrine:* Reaction and after-the-fact forensics are dominant in current cyber operations, reinforcing the desirability of restoring the doctrinal imperative to seize, maintain and exploit the initiative in the cyber domain.
- *DOTMLPF-P Insights/Leadership and Education:* Future Commanders must be just as adept deploying cyber effects as they are delivering physical effects.
- *DOTMLPF-P Insights/Leadership and Education:* Desirable future cyber leader attributes include: A Sense of Urgency, Inquisitiveness: Look at things from not what is but what could be, Discontent with Status Quo, Determination: Never Giving Up, Adaptable to Change, Resilience, Self-awareness of strengths and weaknesses, Creativity, Risk Tolerance, and Ambiguity Tolerance.
- *DOTMLPF-P Insights/Leadership and Education:* Desirable future cyber leader skills include: Mission acumen, Tech ability to understand the threat – and to know and recognize "BS", Team Building, Relationship Building, Recognition of the Big Picture Change Management, Strategy articulation, Influence (without direction authority).
- *DOTMLPF-P Insights/Leadership and Education:* In the coming age of pervasive autonomy, one of the most critical functions of future cyber leaders will be empowerment, not only of subordinates but also of machines: pre-authorized responses will be developed by humans, but executed at machine speed.
- *Cyber Change Management/Culture:* The culture of the cyber security community is 20% innovation, 80% compliance. As compliance security is commoditized, the innovation dimension needs to expand.
- *Cyber Change Management/Ownership:* Legacy leaders are inclined to "let the S-6" address the cyber challenge.

- *Cyber Change Management/Sense of Urgency:* Our Army, culture, and equipment will have to adapt as technology evolves…to operate in this environment, we need to create a sense of urgency.
- *Cyber Change Management/Sense of Urgency:* Leaders must be willing to invest to ensure operations in the cyber domain are current and secure.
- *Cyber Change Management/Sense of Urgency:* Leaders must paint the picture and map out the sequence to accomplish the vision. Some leaders have been reticent to own/address the responsibility of a new dimension of the battlefield

11. Conduct Air-Ground Reconnaissance

How to conduct effective air-ground combined arms reconnaissance to develop the situation rapidly in close contact with the enemy and civilian populations.

Mad Scientist: 2050 Cyber Army Related Observations text

- No observations recorded during the Mad Scientist: 2050 Cyber Army Conference related to this Army Warfighting Challenge.

12. Conduct Entry Operations

How to project forces, conduct forcible and early entry, and transition rapidly to offensive operations to ensure access and seize the initiative.

Mad Scientist: 2050 Cyber Army Related Observations

- No observations recorded during the Mad Scientist: 2050 Cyber Army Conference related to this Army Warfighting Challenge.

13. Conduct Wide Area Security

How to establish and maintain security across wide areas (wide area security) to protect forces, populations, infrastructure, and activities necessary to shape security environments, consolidate gains, and set conditions for achieving policy goals.

Mad Scientist: 2050 Cyber Army Related Observations

- No observations recorded during the Mad Scientist: 2050 Cyber Army Conference related to this Army Warfighting Challenge.

14. Ensure Interoperability and Operate in a Joint, Interorganizational and Multinational Environment

How to integrate Joint, interorganizational, and multinational partner capabilities and campaigns to ensure unity of effort and accomplish missions across the range of military operations.

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/Cyber-Casting:* DoD was originally a driver in the realm of cyber, with dominant key roles in the development of the internet, CPUs, Random Access Memory, Packet Switch Networks, and TCP / IP protocols. That leading role is significantly diminished and dispersed among state and non-state actors.
- *Strategic Context/Cyber Strategies:* The White House International Strategy is aimed explicitly at "engagement with international partners on the full range of cyber issues." It weaves together technical principles (interoperability, stability, reliable access, and security) with values (freedom, respect for property, privacy, and protection from crime) and governance (multi-stakeholder institutions, and self-defense).

15. Conduct Combined Arms Maneuver

How to conduct combined arms air-ground maneuver to defeat enemy organizations and accomplish missions in complex operational environments.

Mad Scientist: 2050 Cyber Army Related Observations

- *DOTMLPF-P Insights/Doctrine:* There is an operational imperative to doctrinally define maneuver in cyberspace but in the absence of physical "position" such schematics for maneuver in cyber are highly complex and dynamic, defined by ever changing avenues of approach that include routers, switches, bridges, and servers that provide data transfer, routing, and storage instructions for the data packets.

16. Set the Theater, Sustain Operations, and Maintain Freedom of Movement

How to set the theater, provide strategic agility to the Joint force, and maintain freedom of movement and action during sustained and high tempo operations at the end of extended lines of communication in austere environments.

Mad Scientist: 2050 Cyber Army Related Observations

- No observations recorded during the Mad Scientist: 2050 Cyber Army Conference related to this Army Warfighting Challenge.

17. Integrate Fires

How to coordinate and integrate Army and JIM fires in combined arms, air-ground operations to defeat the enemy and preserve freedom of action across the range of military operations.

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/Domain Dilemmas:* Cyber effects are far from limited to the cyber domain. Many would argue that the more significant effects of cyber are manifest in its enabling impacts on non-cyber capabilities in the other domains.
- *DOTMLPF-P Insights/Doctrine:* Because of the pervasiveness and ubiquity of cyber activity, deconfliction will be a particular challenge, including deconfliction not only of activity but of purpose.

18. Deliver Fires

How to deliver fires to defeat the enemy and preserve freedom of action across the range of military operations.

Mad Scientist: 2050 Cyber Army Related Observations

- *Strategic Context/Cyber Power:* Strategic cyberwar theory views the adversarial nation as a framework of institutional arrangements instead of a set of military assets and digital networks. These institutional frameworks are likely to be less well defended than the industrial-military complex. However, when attacked or influenced, these frameworks can have an outsized impact on an adversary.

19. Exercise Mission Command

How to understand, visualize, describe, and direct operations consistent with the philosophy of mission command to seize the initiative over the enemy and accomplish the mission across the range of military operations.

Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/Domain Dilemmas:* Consequential time elements can be very small, driving key components of the command decision process toward human-machine solution approaches.
- *Challenge of Cyber/Planning:* Although the cyber domain is a human construct, the complexity of cyber infrastructure together with the speed and global reach of cyber action posits dilemmas to those who would "visualize" cyber-space.

20. Develop Capable Formations

How to design Army formations capable of rapidly deploying and conducting operations for ample duration and in sufficient scale to accomplish the mission.

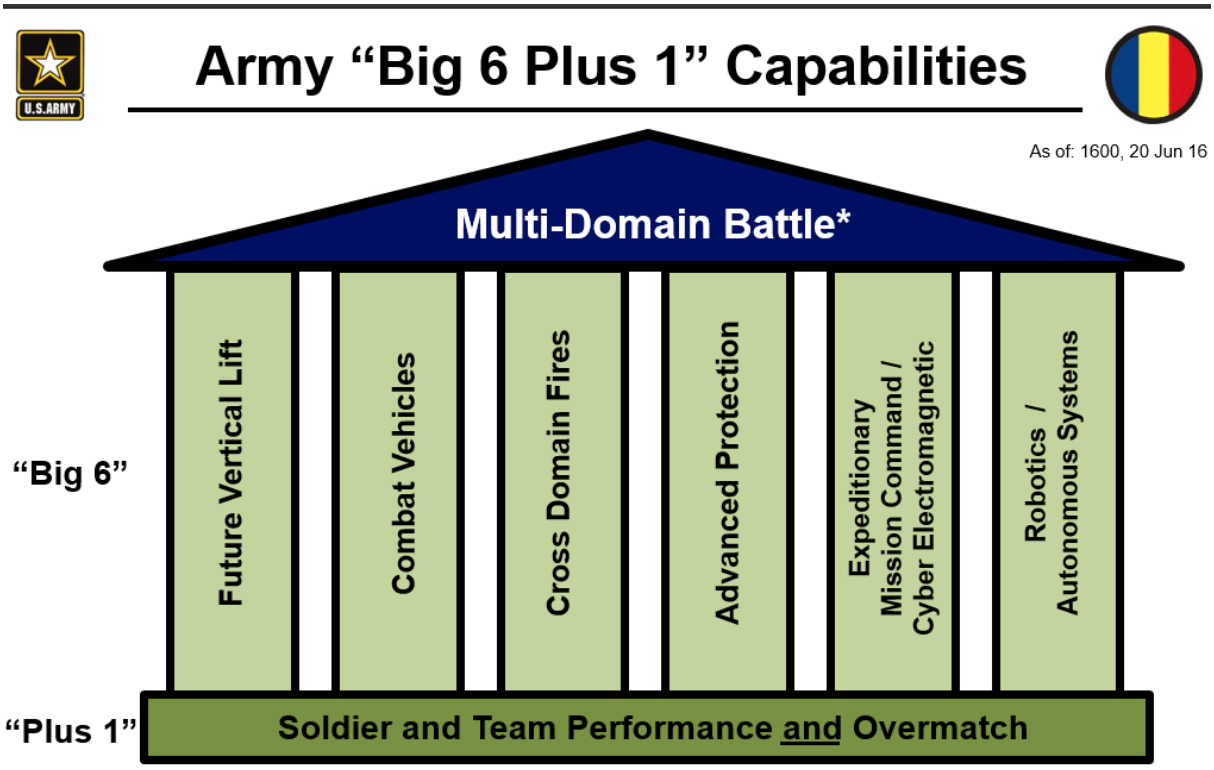
Mad Scientist: 2050 Cyber Army Related Observations

- *Challenge of Cyber/Categorization Conundrum:* In the military field we see it in the convergence of EW, Signal, Information Operations, Intelligence, Public Affairs, and of course: Cyber Operations.
- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* How do organizations account for the fact that technology is both centralizing (e.g., cloud computing) and decentralizing (e.g. device to device communications in the Internet of Things)?
- *DOTMLPF-P Insights/Doctrine:* Doctrine must illustrate cyberspace as a warfighting domain, portraying operations across the land, air, and space domains that will occur by, with, and through the cyber domain.
- *DOTMLPF-P Insights/Organization:* Organizational solutions must account for technology trends that are simultaneously both centralizing and decentralizing.
- *Cyber Futures/Attributes of a Cyber Future:* The Army must account for a cyber future and be capable of operating in a cyber environment that is ubiquitous, volatile, uncertain, complex, and ambiguous.
- *Cyber Futures/Attributes of a Cyber Future:* The Army must operate in an environment featuring *convergence*:
    - **…** between land and cyberspace operations.
    - **…** between time and space as enhanced information and communication technologies decrease the time and expand the reach of cyber actions.
    - … between electromagnetic (EMS) and cyberspace action.
    - … between defensive and offensive cyberspace operations to ensure one function informs the other.
    - … between information management and knowledge management (KM) as large data is leveraged to achieve advantage.

    - … between Army operational and institutional activities, creating an unprecedented level of interaction where operations impact institutional activities and vice-versa.
- *Cyber Futures/Risky Assumptions:* That boundaries and authorities matter. You can't rely on boundaries and authorities to secure the Nation when the enemy doesn't care about how we delineate the problem.

Appendix B-2: Army Science and Technology Challenge Insights

This section of the study aligns important science and technology-related key observations and insights developed during and after the Mad Scientist: 2050 Cyber Army Conference with each of the Army "Big 6 plus 1" Science and Technology Challenges (see figure below). Each observation is tagged by the Quicklook Report framework element (*Challenge of Cyber*, *Strategic Context*, or *DOTMLPF-P Insights, Cyber Futures, or Cyber Change Management*) followed by the relevant report subheading.



1. Multi-Domain Battle

- *Challenge of Cyber/Domain Dilemmas:* Cyber effects can have global reach and effortlessly cross legacy geographic boundaries.
- *Challenge of Cyber/Domain Dilemmas:* Ambiguity makes cyber effects more – rather than less – relevant for adversaries in pursuit of "gray zone" strategies.

- *Challenge of Cyber/Cyber-Casting:* The rate of change in cyber science frustrates forecasting. The unique characteristics of the cyber domain frustrate the predictive power we expect in military theories and strategy. Battle results are indirect, not readily observable and difficult to quantify. Actors are anonymous, and engagements happen at machine speed.
- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* What does "doctrine" mean when the highest form of cyber art is the unprecedented, "zero-day" attack?
- *Strategic Context/Deterrence:* Deterrence is hard to establish. Because there are no international treaties or norms about the use of digital weapons by states, non-state groups or individuals – or even acknowledgment by the U.S. Government that it has ever used them itself -- there are effectively no rules to constrain cyber conflict.
- *DOTMLPF-P Insights/Doctrine:* Doctrine typically draws from theory, but with respect to theory, any future cyber doctrine confronts several challenges, including no dominant theory to describe cyber's bridge between the physical, cognitive, and moral dimensions of conflict; physical metaphors that do not match the cyber domain, and the growth of capabilities that far outpaces relevant theory and doctrine.
- *DOTMLPF-P Insights/Material:* Internet of things, centralization and decentralization, connectivity, and smart grid arrays will define cyber technology developments.
- *DOTMLPF-P Insights/Material:* Sentient Tools are "what comes next" and emerge from a base of computational, sensing and communications technologies that have been advancing for over the last 50 years. Sentient Tools will drive the next phase of development of computational systems, smart cities and environments, autonomous systems, artificial intelligence, big data and data mining, and an interconnected system in the Internet of Things (IoT).
- *Cyber Change Management/Vision:* Future cyber vision must account for inevitable ubiquity and pervasiveness of cyberspace. It must feature *unity of cyberspace*: for the battlefield of 2050 the appropriate relationships, doctrine and arrangements and concepts must be built jointly between industry, militaries of different countries, and inter agency partners.
- *Challenge of Cyber/Planning:* For the United States, reaction (and defense) is decentralized; action (and offense) tends to be highly centralized. The offense / defense dynamic is also symmetric to our adversaries, who frequently decentralize their offensive operations.
- *Challenge of Cyber/Categorization Conundrum:* Cyber – and the digitization that underlies it – is ubiquitous and impacts everything. This ubiquity confounds our traditional approaches to categorization in almost every field, with a "boundary busting" impact that diffuses the distinctions between civil and military action,

between the physical / informational / moral dimensions of conflict, and across the diplomatic, informational, military, and economic (DIME) elements of power.

- *Challenge of Cyber/DOTMLPF-P "Through the Looking Glass":* How do we plan for cyber infrastructure considerations that are global and external to military control?
- *Strategic Context/Deterrence:* Deterrence options may include sanctions, indictments, cyber retaliatory options, and even the threat of kinetic measures. The ubiquity of cyberspace weapons and the difficulty of attribution in cyberspace means that our traditional deterrence options will not always succeed against a variety of cyber threats.
- *DOTMLPF-P Insights/Doctrine:* There is an operational imperative to doctrinally define maneuver in cyberspace but in the absence of physical "position" such schematics for maneuver in cyber are highly complex and dynamic, defined by ever changing avenues of approach that include routers, switches, bridges, and servers that provide data transfer, routing, and storage instructions for the data packets.
- *Challenge of Cyber/Categorization Conundrum:* In the military field we see it in the convergence of EW, Signal, Information Operations, Intelligence, Public Affairs, and of course: Cyber Operations.
- *Cyber Futures/Risky Assumptions:* That boundaries and authorities matter. You can't rely on boundaries and authorities to secure the Nation when the enemy doesn't care about how we delineate the problem.

2. Future Vertical Lift

- No observations recorded during the Mad Scientist: 2050 Cyber Army Conference related to this Army Science and Technology Challenge.

3. Combat Vehicles

- No observations recorded during the Mad Scientist: 2050 Cyber Army Conference related to this Army Science and Technology Challenge.

4. Cross Domain Fires

- *Challenge of Cyber/Domain Dilemmas:* Cyber effects are the principal bridge between the physical and cognitive dimensions of conflict, and – through information warfare – impact the moral domain (the domain of belief).
- *Strategic Context/Deterrence:* Cyber attackers are hard to identify with certainty, and the evidence cannot be made public.

- *Challenge of Cyber/Domain Dilemmas:* Cyber effects are far from limited to the cyber domain. Many would argue that the more significant effects of cyber are manifest in its enabling impacts on non-cyber capabilities in the other domains.
- *DOTMLPF-P Insights/Doctrine:* Because of the pervasiveness and ubiquity of cyber activity, deconfliction will be a challenge, including deconfliction not only of activity but of purpose.
- *Strategic Context/Cyber Power:* Strategic cyberwar theory views the adversarial nation as a framework of institutional arrangements instead of a set of military assets and digital networks. These institutional frameworks are likely to be less well defended than the industrial-military complex. However, when attacked or influenced, these frameworks can have an outsized impact on an adversary.

5. Advanced Protection

- *Strategic Context/Cyber Power:* The most capable and least risky future military is one in which digital technologies enhance capabilities but are not uniquely critical vulnerabilities.
- *DOTMLPF-P Insights/Material:* Many of our current security vulnerabilities are by design; over time many of these design flaws can be corrected. Several disruptive materiel solutions may mitigate some cyber vulnerabilities, including for example quantum sensing and quantum communication, Read-Only Memory (ROM), and security models that mimic biological systems
- *DOTMLPF-P Insights/Facilities:* The centralization trend of some cyber technologies such as cloud computing positions those central facilities as significant targets for either cyber or kinetic attack.

6. Expeditionary Mission Command/Cyber Electromagnetic

- *Challenge of Cyber/Planning:* Many cyber intelligence tools are forensic in nature.
- *Challenge of Cyber/Planning:* The greater the reliance on advanced cyber capabilities – both as direct weapons and as enablers for conventional capabilities – the greater the potential disruption, diversion, and destruction that adversaries can create via malicious cyber activities in the future.
- *Strategic Context/Cyber Strategies:* The Electronic Warfare function lacks a coherent vision and strategy at both DoD and Army levels.
- *Strategic Context/Cyber Power:* To practice effective mission command, sustain the forces, provide critical intelligence, and communicate over the horizon, a nation must be a cyber and space power.
- *DOTMLPF-P Insights/Doctrine:* Doctrinal “levels of war” of war pose unique challenges in the cyber domain, with tactical actions having global reach, and

significant “sub-platform warfare” that can be isolated to singular platforms or pervasive, damaging lower layer infrastructure like Operating Systems (OSs), BIOS, hardware, hard drives, and memory disks, and thereby crippling widespread capabilities and services that depend on these lower layers.

- *DOTMLPF-P Insights/Material:* Electromagnetic Pulse (EMP) Vulnerabilities. Near-peer competitors like Russia, China, North Korea, and Iran all make EMP attack a complementary part of their cyber doctrine.
- *DOTMLPF-P Insights/Doctrine:* Doctrine must illustrate cyberspace as a warfighting domain, portraying operations across the land, air, and space domains that will occur by, with, and through the cyber domain.
- *DOTMLPF-P Insights/Organization:* Organizational solutions must account for technology trends that are simultaneously both centralizing and decentralizing.
- *Cyber Futures/Attributes of a Cyber Future:* The must operate in an environment featuring convergence:
    - **…** between land and cyberspace operations.
    - **…** between time and space as enhanced information and communication technologies decrease the time and expand the reach of cyber actions.
    - … between electromagnetic (EMS) and cyberspace action.
    - … between defensive and offensive cyberspace operations to ensure one function informs the other.
    - … between information management and knowledge management (KM) as large data is leveraged to achieve advantage.
    - … between Army operational and institutional activities, creating an unprecedented level of interaction where operations impact institutional activities and vice-versa.

7. Robotics and Autonomous Systems

- *DOTMLPF-P Insights/Leadership and Education:* In the coming age of pervasive autonomy, one of the most critical functions of future cyber leaders will be empowerment, not only of subordinates but also of machines: pre-authorized responses will be developed by humans, but executed at machine speed.

8. Solder and Team Performance and Overmatch

- *DOTMLPF-P Insights/Training:* Future training can leverage simulation or gaming technology aided by artificial intelligence that replicates real terrain, physical structures, and social interaction in cyberspace.
- *DOTMLPF-P Insights/Training:* Cyber capabilities must be incorporated into exercises in order to establish credibility with the broader operational force.

- *DOTMLPF-P Insights/Training:* Cyber technologies are accelerating the process of 'cognitive off-loading' in humans, whereby computational / cognitive tools shorten our attention spans and memory, impacting education and learning.
- *DOTMLPF-P Insights/Personnel:* To get ready for 2050, the Army needs to stop recruiting at shopping malls. Recruit at STEM programs; find cyber aptitude in middle and high school and develop relationships that support and encourage youth to serve in the Army.
- *Cyber Change Management/Culture:* There is an important role for meta-cognition: the ability to recognize the ideas we already hold.
- *Challenge of Cyber/Domain Dilemmas:* Consequential time elements can be very small, driving key components of the command decision process toward human-machine solution approaches.

APPENDIX D:

Appendix C: Survey Results

The 2050 Cyber Army Survey Data

The 2050 Cyber Army Analysis Team collected and analyzed responses to a survey conducted prior to, during, and immediately after the Conference. Survey participants were asked to name and describe a high-priority emerging technology and evaluate its impact relative to Army TRADOC Technology areas and Warfighting Challenges. In total, 16 participants responded to the survey, providing 33 individual responses. The overall results of the effort are provided here. The remainder of this appendix provides each technology nominated by respondents, the frequency with which each technology appeared by TRADOC Technology Line of Effort (LOE), and the frequency with which each respondent deemed the technology to be relevant to assisting in solving a particular Warfighting Challenge.

Technologies Nominated by Respondents

Survey respondents nominated fourteen separate cyber-related areas as having a high impact for the U.S. Army going forward. These technology areas are:

- Risk Management Framework Implementation: Implementation of the Risk Management Framework (RMF) for DoD Information Technology (IT) as it applies to Armament Systems.
- KEEL Technology: KEEL Technology allows domain experts to put their reasoning (decisions, judgment, system behaviors) into applications. Autonomy (or semi-autonomy), diagnostics/prognostics, policies to aid the warfighters (decisions, ethics, safety, etc).
- GPS Spoofing: Ability to subtly misdirect vessels, air and spacecraft with under $5K worth of equipment – as well as defenses against these capabilities.
- Bitcoin Interacting with Machines: Code that will allow any GPIO device, Iot Device or networked machine to interact with the Bitcoin Blockchain for both payment operated control, dynamics, and diagnosis of device, data transfer and records of machine use.
- Area Defense of Individual Cyber Target: Targeting of cyber actor's area of interest in spite of "defended" cyber targets.
- BitCongress – Decentralized Direct Democracy: A purely peer to peer version of electronic vote would allow online votes to be sent directly from another without going through a central voting register.
- Root Causes for Cyber-Attacks: The fundamental causes for each cyber-attack in each application (Software & Hardware) needs to be knownThe root causes for each kind cyber-attack may not change with time much although the cyber technologies will have dramatic changes from macro to micro to nano.
- Meet Your Army: Synchronization of outreach efforts under the umbrella of the Army PAO.
- Student-Centric Subject Matter Expert Network: Development of interested students and

student-led organizations on campuses to develop accessible subject matter expertise, knowledge, capabilities, and other leading ideas for cyber.

- E-Intern Program for Army Cyber: Adaptation of Army Education to allow our young people to become real or electronic interns and study outside of the Army to learn cyber skills. Army Cyber students must learn through internships, study outside the Army programs.
- Makers Revolution: The Army needs to invest in an understanding of how to leverage the maker revolution as critical aspect of our innovation effort.
- Critical Thinking Skills: Reliance on Big Data Analytics means our ability to make bad decisions may increase. We have to ensure that our biases are checked will in advance, and that means that we have to invest much more heavily in decision sciences research/understanding.
- Bachelor of Science Degrees in Cybersecurity: It is unrealistic to expect colleges and universities to produce junior cybersecurity professionals who are completely knowledgeable in all of the current technological tools and ready to instantly respond to a system intrusion. The expectation should be instead that higher education will produce graduates who understand cybersecurity basics, who can see the big picture of how their efforts fit into those of the organization.
- Enemy Intent/Decision Voice Detection: Software modification so that the intent of our enemy could be determined through voice recognition.
- Spearphishing Trap: Funnel spearphishing attackers into honeypots. Reduce user email vulnerability to spearphishing. Reduce resources devoted to spearphishing remediation. Solution consists of a suite of technologies which combines an improved email interface, federated identity, 2 factor authentication and honey pot.
- Army Nexus: Use of community technology l to create a network of school robotics and computer clubs. The central idea is to create a means to connect members of the military cyber community to young people who are interested in cyber challenges.
- Industry Collaboration: DoD to allow for the establishment of specific contracts with companies in critical industries to allow the sharing of information regarding Cyber threats and attacks to include those threats and attacks of which are classified.
- E-Waste: Every year the Army and DoD generates millions of pounds of e-waste. In the event of a conflict or war by 2050 our supply chain for obtaining raw materials could be disrupted to the extent that we are unable to mass produce new technologies. Having effective and efficient ways of recycling current computers or recovering e-waste which has ended up in a landfill could mean the difference between being able to win a cyber war or not
- Evolving Officer Education: By 2050 the Army should look to integrate more foreign students or require of its own students a minimum of one year studying abroad, especially in the Cybersecurity fields. This will ensure that our future leaders better understand cultural nuances, especially within the Cybersecurity field.
- Continuous Learning Degrees: By the year 2050 it may be accepted that students never fully graduate from a College or University. Their degrees may Degrees would replace the need for certifications; certifications would be included in the conferment and sustainment of a degree.
- STEM Summer Camps: In order to inspire the youth of today to find interest in STEM subjects, the Army should sponsor STEM summer camps for youth.

APPENDIX D:

- Separation of Applications from OS: The Army should begin immediately working towards the separation of applications from the operating system. By 2050, applications will all run similar to how thin applications and/or web based applications run today.
- De-regionalization and Mesh and Trust Creation: The future of IT in the year 2050, especially for the DoD, is not in large centralized data centers. Rather, in a mesh of smaller, local data centers with a focus on creating trusts between the smaller data centers.
- Data Management: Text By the year 2050, greater importance will be given to data management. The Army (and DoD) will come to the realization that not all data has the same value and not all data should be treated the same. Some data will have multiple backups and have high availability and other data will only one backup and have low availability.
- Intelligent Data Sharing: In the Army of 2050, information may be stripped of the identities of the people who created it or were involved in it and made public to the entire Army.
- Evolving the RF and EW Environment: By the year 2050 the RF and EW battle space will have advanced significantly. Included in the crew systems of all HMMWVs, MRAPs, TANKs, etc. will be electronics which detect all wireless signals in their area. This information (frequency and signal strength) will be relayed back to a central processing computer which combines all of the information into a common operating picture (COP) of the RF battlespace.
- Evolution of Service Desks: By the year 2050, there will be one unified DoD Cyber helpdesk system. All of the major centrally located IT service desks within the DoD will be dismantled. Tier I, II, and III personnel will all be located on each base/post/camp/station but will operate in a virtual mesh.
- Identity and Profile Management: By the year 2050, there will be a DoD wide profile and identity management system. All users who need access to any DoD network will have all of the accesses they need on one ID card. There will be no separate tokens for SIPR and no separate ID cards for people who have multiple personas such as military reservist/civilian or military reservist/contractor.
- Training and Unifying the Cyber Force: The creation of a Cyberforce could be extremely expensive and problematic. Instead, by the year 2050, the Army and the DoD should focus on ensuring that there is better collaboration & unification of IT between all of the Service
- Cyber Theory: Cyber branched officers are not cognizant of the sister branches Signal, Intelligence, EW, Space, etc. Training of cyber officers should change, growing cyber officers able to bridge these gaps and make this capability an enabler for Maneuver Commanders.
- GDELT and JIGSAW: Tools to assess micro-level sociocultural reactions to events.

Nominated Technologies by Army TRADOC Science and Technology Line of Effort
The largest single S&T category of S&T survey responses was “other,” with ten responses, closely followed by LOE 7 (Human performance enhancement) with nine responses. LOE 6 (Accelerated Data to Decision also featured prominently with 6 responses. “Other”

responses focused on education and cultural changes to enable the full realization of cyber-power within the future Army.

S&T Line of Effort	Responses
LOE 1: Mobile Protected Systems	1
LOE 2: Improve Lethality and Effects	3
LOE 3: Logistics Optimization	1
LOE 4: Aviation	1
LOE 5 Cyber Electromagnetic Activities	3
LOE 6 Accelerated Data to Decision	6
LOE 7 Human Performance Enhancement	9
LOE 8 Robotics	0
Other	10

Nominated Technologies and Number of Times Respondents Linked to Warfighting Challenges.

Warfighting Challenge	Times Applicable
Develop Situational Understanding	18
Shape the Security Environment	14
Provide Security Force Assistance	4
Adapt the Institutional Army	15
Counter Weapons of Mass Destruction	5
Homeland Defense	10
Conduct Space and Cyber Electromagnetic Operations	8
Enhance Training	11
Improve Soldier, Leader, and Team Performance	9

APPENDIX D:

	Develop Agile and Adaptive Leaders	10
	Conduct Air-Ground Reconnaissance	2
	Conduct Entry Operations	2
	Conduct Wide Area Security	3
	Ensure Interoperability and Operate in a JIIM Environment	3
	Conduct Combined Arms Maneuver	2
	Set the Theater, Sustain Operations, and Maintain Freedom of Movement	3
	Integrate Fires	1
	Deliver Fires	2
	Exercise Mission Command	5
	Develop Capable Formations	2

Appendix D: Collection and Assessment Methodology

This Appendix describe the collection, organization, and assessment of data, information, and knowledge for the ***Mad Scientist 2016 Conference: The 2050 Cyber Army***, including associated papers, speakers, conference discussions, and survey tool responses. Our overall approach to data collection and analysis is captured in Figure 1 below.

Collection and Assessment Topic	Description
Background	What is the situation being studied?
Purpose	Why is this study being conducted?
Key Tasks	What tasks must be accomplished, and who will do them?
End State and Deliverables	What will this effort produce? What is the deadline for the project?
Scope	What are the limits of this collection effort? Who will be involved?
Concept	What is the scale of effort and what areas must be examined? Who will conduct the study? What is the time frame for the study?
Research Questions	What are the issues to be examined? What questions must be asked to examine those issues? Optionally, hypothesize what you are trying to confirm or deny.
Key Personnel and Organizations	Who can answer these questions? Develop a list of key personnel to be interviewed.
Methodology	How will the study be organized? How will various teams interface?
Reference Material	What will be the primary documents of reference? How will they be applied in the study?
Data Collection Procedures	What quantitative and qualitative data must be collected, and how and when?

Data Management Procedures	How will collected data be managed? Who will have access to the data and at what stages of collection and analysis? Who has release authority? What are the classification procedures?

Figure 1: Overall Approach to Data Collection and Analysis

Background

On 13-14 September, United Sates Army TRADOC G2 conducted *The 2050 Cyber Army Conference* in partnership with the Army Cyber Institute. This event explored the requirements for the Army's 2050 cyber force. This conference was part of a larger United States Army TRADOC *Mad Scientist Series* in support of the overall Army *Campaign of Learning*.

Purpose

This event was designed to support the broader Army Mad Scientist initiative goals to continuously adapt, innovate, and allow for broader engagement in problem solving within the far future of armed conflict. This conference focused on exploring two lines of effort in *The Army Cyberspace Strategy for Unified Land Operations 2025*. These were:

- Line of Effort 1, Build the Workforce. This LOE constitutes the Army's main effort and it consists of several objectives. First, the Army must recruit, develop, and retain the Cyberspace Workforce. It must then educate the Total Force, including military, Department of the Army (DA) Civilians, and contractors in all three components (Active, Guard, Reserve). Then, it must train and certify the Total Force.
- Line of Effort 5, Partnerships. No single organization can resolve all cyber challenges. The Army must work with partners to achieve its vision. The Army also must partner with organizations across DoD and other United States Government agencies to enhance Army cyberspace operations as a member of an integrated team. These partners harness academic, industry, and allies' capabilities.

This Collection and Assessment Methodology describes how the analysis team collected and assessed the event data to provide observations and insights captured in subsequent Quicklook and Final Reports.

Key Tasks

Key tasks for this collection and assessment effort are derived from the 2050 Cyber Army Mission Analysis Paper and included:

- Prepare for the *2050 Cyber Army Conference* by developing a collection and assessment protocol (due 12 September 2016)
- Read the *Army Cyberspace Strategy for Unified Land Operations 2025*, and read and assess research papers developed in preparation for the conference
- Observe briefings and panel discussions during the event and collect and organize the results of each phase of the conference
- Assess the results of the *2050 Cyber Army Conference*
- Generate a Quicklook Report for the TRADOC G2 (due 17 October 2016)
- Write a Technical Report with the results of the 2050 Cyber Army Conference that further refines our understanding of the role of cyber and needed cyber proficiencies required in the future Operating Environment (FOE) and the underlying technology evolution
- Finish report within 45-60 days following event (due NLT 7 November 2016)
- Support HQ TRADOC analytical team, by collecting notes and developing observations and insights during the event and from live stream questions and comments and providing consolidated insights to forward TRADOC G-2 personnel at event, to aid in updates and briefings to senior U.S. Army personnel.

End State and Deliverables

The observations and insights generated in accordance with this collection and assessment methodology will enable the delivery of key insights for senior Army leaders to support the *Army Cyberspace Strategy for Unified Land Operations in 2025* and to assist in TRADOC G-2s understanding of the future operating environment through 2050. The new knowledge resulting from this analytic effort is designed to support the Army Campaign of Learning, Army Force 2025 Maneuvers, and capability development efforts.

All data were captured and assessed, and initial observations and insights were refined and presented in a Quicklook Report (due 17 October 2016). This Technical Report builds on the framework set out in the Quicklook Report. It provides a more detailed description of the full set of conference results, consolidating relevant data from the call for papers, from conference presentations and panel discussions, relevant survey data, and other research material available to the analysts and was delivered on 22 October 2016.

APPENDIX D: COLLECTION AND ASSESSMENT METHODOLOGY

Scope

This Collection and Assessment Methodology was designed to capture and refine the set of data, information, and knowledge developed for and during the September 2016 *2050 Cyber Army Conference*, subject matter expert papers developed in preparation for the conference, and several relevant, contemporary studies related to the future cyber environment and how the future Army may operate and fight within cyberspace.

Concept

The concept to collect and assess information generated over the course of *the 2050 Army Cyber Conference* included the following elements:

- Survey the body of Army Cyber Strategy documentation and other materials related to the future of cyberspace and cyber operations.
- Review the submitted conference papers made available by the TRADOC G2.
- Collect notes from the assessment team captured over the course of the *2050 Cyber Army Conference* using a structured set of information elements related to each of the research questions (see **Research Questions** and **Methodology, *phase 2*** below).
- Assess the results of the *2050 Army Cyber Conference.*
- Write a Technical Report with the results of the *2050 Army Cyber Conference*, with specific recommendations to the TRADOC plan.
- Finish Technical Report within 45-60 days following event.
- Support HQ TRADOC analytical team, through collecting insights via live stream of conference and associate captured insights to f.1-6 (questions); provide consolidated insights to forward (G-2 personnel at event) to aid the G-2 in briefs to the senior Army personnel present during event.

Research Questions

The event intended to address three research questions that will drive the note-taking methodology, continuous analysis, and observations and insights development. These questions included:

1. What does the cyber environment look like in 2040-2050 (how will cyber influence the environment and the population? What will connecting look like / what will they connect to? What are the drivers influencing this or not)?
2. How do we build an Army Cyber Force that can dominate the cyber domain in the context of the multi-domain battle concept to gain a position of relative advantage?

3. How can we build shared goals and expectations as well as develop an understanding of roles and responsibilities in order to build and maintain partnerships with U.S., and international academia, industry, defense departments/ministries and other agencies to enhance cyberspace operations? What new ideas should we be considering?

Key Personnel

The analytic effort was undertaken by Mr. David Fastabend, Mr. Greg Gardner, and Mr. Jeff Becker, contracted to undertake this analysis. The conference note taking and observation development team also included LTC Kristian Muench, MAJ Christopher Deale, Mr Tom Schmidt, Ms Catherine McNear and Mr. Matt Santaspirt of the TRADOC G-2 office.

This collection and assessment methodology also relied on close collaboration with several important partners to ensure the full set of data was collected from the event and that the observations and insights were received by Army TRADOC leadership in an organized and timely manner. These key personnel included:

- Mr. Joel Lawton, TRADOC G2: Overall study integration and senior leader support
- Ms. Allison Winer, Mad Scientist SME and Ms. Kira Hutchinson, TRADOC G2: Real-time insight and observation development
- Mr. Gary Retzlaff, TRADOC G2: Survey tool data and results

Methodology

The methodology used to assess data and information collected over the course of the *2050 Cyber Army Conference* occurred over the following four phases.

In **Phase 1** (Pre-Conference Preparation), the team conducted a comprehensive review of applicable literature, including prior Mad Scientist study reports, the reference material cited at Appendix E of this report. The team reviewed papers submitted under the associated Call for Papers. The team also reviewed relevant research material such as the material cited at Appendix B of this report. Each of these external sources was examined for pertinent facts, observations, and insights related to the study research questions and were included in a running observations register.

The team formulated the Quicklook and Final Report structures by examining the overarching hypothesis, supporting research questions, and developed a report structure that communicated key ideas from across all sources in a logical and useful way (see phases 3 and 4 below for details).

APPENDIX D: COLLECTION AND ASSESSMENT METHODOLOGY

In **Phase 2** (Conference Execution), two members of the team (Fastabend; Gardner) were located on-site and attended all Conference proceedings. The conference was designed around briefings and panels designed to explore issues or topics important to the future Cyber Army. They were intended to spark discussion among group participants about how cyberspace may evolve out to 2050 and the implications of these changes for the Army in terms of its cyber structure and functions.

The note-taking and observation development team conducted continuous assessment and synthesis of the proceedings. In order to capture conference presentations and discussion sufficient to address the research questions, the team took detailed notes and conducted continuous assessment. This continuous assessment was based on several information elements associated with each of the research questions (derived from section 4.e., *Mission Analysis: The 2050 Cyber Army*):

1. What does the cyber environment look like in 2040-2050 (how will cyber influence the environment and the population? What will connecting look like / what will they connect to? What are the drivers influencing this or not)?
    a. Element 1-a: What are major assumptions about the cyber domain through 2050?
    b. Element 1-b: What are major assumptions about the relationship between the cyber domain and other warfighting domains?
2. How do we build an Army Cyber Force that can dominate the cyber domain in the context of the multi-domain battle concept to gain a position of relative advantage?
    a. Element 2-a: What shape might a future cyber army take?
    b. Element 2-b: For far-future Army planning, what can we know or need to know about:
        i. Defending DoD networks, systems and information to 2050?
        ii. Defending U.S. and its interests against cyber-attacks to 2050?
        iii. Providing integrated cyber capabilities to support military operations and contingency plans to 2050?
3. How can we build shared goals and expectations as well as develop an understanding of roles and responsibilities in order to build and maintain partnerships with U.S., and international academia, industry, defense

departments/ministries and other agencies to enhance cyberspace operations? What new ideas should we be considering?

a. Element 3-a: What industry partners should the Army consider to address cyber challenges through 2050?

b. Element 3-b: How can the Army encourage and work with a larger cyber Community of Interest in order to:

   i. Drive cyberspace-related innovation across the Army and;

   ii. Understand and develop key baseline cyber skills that every Soldier will need in 2050?

The team listened to each panel and presentation, and collected notes based on this method. As necessary, the team engaged with conference participants both during and after the conference to further refine and develop ideas. The team will collected briefings for reference during phase 3 of the methodology. The team integrated written materials from these panels and briefings as the foundation the Quicklook and Technical Report development and writing efforts as well.

In Phase 3 (Quicklook Report Development) the team developed an initial synthesis of key findings related to the research questions. The Quicklook Report was organized according to several broad thematic areas, including: the challenge of cyber; strategic context, DOTMLPF-P insights, cyber futures, and cyber change management and will focus on surfacing and refining important issues described in the papers, the 2050 Cyber Army Conference presentations and proceedings, and the survey results.

The team will deliver a *2050 Cyber Army Quicklook Briefing* in Microsoft Word format. It will describe emerging themes in order to support AAR development for the wider TRADOC G2 effort.

In Phase 4 (Technical Report Construction) the team constructed a technical report that informs the Army campaign of learning. This report was built from the major structural elements of the Quicklook, adding depth and detail to the five thematic areas. Moreover, the report providing context about how the major observations and insights were derived as well as how they might be effectively incorporated by the Army, particularly in terms of options for future learning, going forward.

Reference Material

Primary studies and other materials associated with the study is cited in the reference section of the final technical report (Appendix E).

APPENDIX D: COLLECTION AND ASSESSMENT METHODOLOGY

Data Collection Procedures

The team conducted real-time collection management to ensure accurate and complete impressions of the event, to ensure that all notes could be shared between team members. Each set of notes was collected and stored in Microsoft Word files on a Microsoft OneDrive shared file system. These summaries were also shared and saved on two independent computers for continuity of operations.

The notes and analysis team held daily collaboration sessions to share key insights from the day's work and to begin to identify key and recurring themes. This disciplined and methodical cataloguing of summaries and other documents, coupled with the verbal discourse during the event enabled timely analysis of conference proceedings and the development of the observations and insights for the Quicklook and Technical Reports.

Data Management Procedures

Data collected during the event was managed individually be the team members. The information was shared via Google Gmail accounts and Microsoft OneDrive file structures. Only note and analysis team members had access to the data. Data release is managed by Mr. Fastabend, who provided TRADOC G2 raw collected data and analytic materials when requested. This material is unclassified, but until publicly released, is sensitive in nature. As such, it has not been shared except between the team members and between the team and TRADOC G2 authorities.

Appendix E: References

Dr. Dave Alberts, Comments on the Mad Scientist Panel: “Challenges and Opportunities in Partnerships”, Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.

Graham T. Allison and Robert Blackwill, “America’s National Interests: A Report from the Commission on America’s National Interests” July 2000.

Marene Allison and Scott Stevenson, Comments on the Mad Scientist Panel: “Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Dr Gillian Andrews, Senior XD Consultant, ThoughtWorks; Comments on the Mad Scientist Panel: “Educating the Cyber Force of 2050”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Margaret Andrews, “The Future of On-Campus Higher Education?” StratEDgy (blog on strategy and competition in higher education at https://www.insidehighered.com/blogs/stratedgy/future-campus-higher-education), 31 March 2015.

Dr. Marni Baker Stein, Chief Innovation Officer, University of Texas System; “Educating the Cyber Force of 2050”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

D. McMahon; R. Rohozinski. “The Dark Space Project.” Defence R&D Canada - Centre for Security Science, Ottawa ONT (CAN). 1 July 2013.

LTG Edward Cardon, Commanding General, US Army Cyber Command; “2014 Green Book: Army Cyber Command and Second Army”, 30 September 2014.

Lieutenant General Edward Cardon; Former Commander, U.S. Army Cyber Command and Second Army, “The Future of Army Maneuver – Dominance in the land and Cyber Domains”.

Bill Cheswick, Visiting Scholar, University of Pennsylvania, Comments on the Mad Scientist Panel: “Community of Hackers and Makers and Innovative Thinkers”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Bryan Clark, Mark Gunzinger, “Winning the Airwaves: Regaining America’s Dominance in the ElectromagnetIc Spectrum” CSBA Report, 2015.

APPENDIX E: REFERENCES

COL(R) Alex Cochran, BAE; Comments on the Mad Scientist Panel: “Who Defends the Nation in 2050?” Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.

Greg Conti, Director Information Security Research, IronNet CyberSecurity; Comments to the Mad Scientist Panel: “Community of Hackers and Makers and Innovative Thinkers”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Jamey Cummings, Comments on the Mad Scientist Panel: “Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Kathleen Curthoys. “New Commander takes Lead at Army Cyber Command.” Army Times, October 14, 2016 at https://www.armytimes.com/articles/new-commander-at-army-cyber-command.

Charlie Dunlap, “ ’Cybervandalism’ or ‘Digital Act of War’? America’s muddled approach to cyber incidents won’t deter more crises” at https://sites.duke.edu/lawfire/2016/10/30/cybervandalism-or-digital-act-of-war-americas-muddled-approach-to-cyber-incidents-wont-deter-more-crises/, 30 October 2016.

Jeffrey A. Eisenach, Claude Barfield, James K. Glassman, Mario Loyola, Shane Tews. “An American Strategy for Cyberspace” American Enterprise Institute, June 2016.

Zach Epstein, “How to Find the Invisible Internet,” BGR.com on 20 January 2014 at http://bgr.com/2014/01/20/how-to-access-tor-silk-road-deep-web/.

Mr. David Fastabend and Mr. Jeff Becker, Mad Scientist Conference 2016: Strategic Security Environment in 2025 and Beyond (October 2016).

Ben FitzGerald, Peter L. Levin, and Jacqueline Parziale, “Open Source Software and the Department of Defense”, Center for A New American Security, August 2016.

Sydney J. Freeburg, Jr. “Electronic Warfare: We Have the Technology – but Not a Strategy”, Breaking Defense, 02 Dec 2015.

Sydney J. Freeburg, “Army Wargames Hone Battlefield Cyber Teams,” Breaking Defense, 07 November 2016.

MG Malcolm Frost, Chief of Public Affairs, US Army; Response to Q&A at “Opening Comments / Stage Setting” Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

BG(P) Patricia Frost, Director of Cyber, US Army, “Opening Comments / Stage Setting” Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

APPENDIX E: REFERENCES

Anna Mulrine Grobe, “The Technologist convincing the Pentagon to Love Hackers.” Christian Science Monitor Online, Oct. 21, 2016.

Michael V. Hayden, The Future of Things “Cyber,” 5 STRATEGIC STUD. Q. 3, 4 (2011).

Jason Healy, “The Five Futures of Cyber Conflict and Cooperation”, Atlantic Council Cyber Statecraft Initiative, 2011.

LTG(R) Rhett Hernandez, Mad Scientist input, October 2016.

Kelly Jackson Higgins, “The Kevin Durant Effect: What Skilled Cyber Security Pros Want”, Information Week Dark Reading, 19 October 2016 at: http://www.darkreading.com/vulnerabilities---threats/kevin-durant-effect--what-skilled-cybersecurity-pros-want-/d/d-id/1327215.

CPT Kurtis M. Hout Jr, 1st Combat Aviation Brigade, 1st Infantry Division, Fort Riley, Kansas; “Maneuvering in an Intelligent Direction: 2 Army Cyber Dilemma’s Which Need to be Addressed by the Mid-21st Century”, paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.

Dr Kamal Jabbour and Major Jenny Poisson, “Cyber Risk Assessment in Distributed Information Systems,” The Cyber Defense Review (Spring 2016).

Brian David Johnson, Futurist and Fellow, Frost & Sullivan; “The Coming Age of Sentient Tools: When Our Tools are Aware, Social, and Think”, Frost & Sullivan 2016.

Brian David Johnson, ‘A Widening Attack Plain: Initial Cyber Threat-casting Report out for Mad Scientists”, Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Dr. Jan Kallberg, “Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations,” The Cyber Defense Review (Spring 2016).

Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” International Security (Fall 2013).

Lucas Kello, “Private Sector Cyberweapons: Strategic and Other Consequences.” (June 2016), Social Science Research Network.

Cameron F. Kerry, “Bridging the Internet-Cyber Gap: Digital Policy Lessons for the Next Administration,” Center for Technology Innovation at Brookings, July 2016.

Brian Krebs. “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage.” Krebsonsecurity blog 21 Oct 2016 at https://krebsonsecurity.com/2016/10/hacked-

cameras-dvrs-powered-todays-massive-internet-outage/.

James Lewis, “Laying Down a Marker”, thecipherbrief.com, October 23, 2016.

Martin C. Libicki, “Cyberspace is Not a Warfighting Domain”, I/S: A Journal of Law and Policy for the Information Society.

Joseph Marks. “The US Needs One Cyber Defense Agency—Not Three, a Top NSA Official Says.” defenseone.com, 20 October 2016.

Alexander McCoy, Best Defense Guest Columnist. “We Need a Cyber Corps as a Fifth Service.” Best Defense Blog, Foreign Policy Magazine, 18 March 2015.

Robert M. McDowell and Gordon M. Goldstein. “The Authoritarian Internet Power Grab.” The Wall Street Journal, 25 October 2016 at http://www.wsj.com/articles/the-authoritarian-internet-power-grab-1477436573.

GEN Mark Milley; Chief of Staff, U.S. Army. “The Army Cyberspace Strategy for Unified Land Operations.” January 2016.

GEN Mark Milley; Chief of Staff, U.S. Army. “Changing Nature of War Won't Change Our Purpose.” Army.mil, October 4, 2016.

President Barack Obama. “National Security Strategy”. 2015.

Stephen O’Grady. “The Software Paradox: the Rise and Fall of the Commercial Software Market”. O’Reilly Media Inc, March 2015.

Phillip Perry, “Cognitive Off-loading: How the Internet is Changing the Human Brain”, Big Think, http://bigthink.com/philip-perry/cognitive-offloading-how-the-internet-is-changing-the-human-brain, 24 Aug 2016.

Andrew Plato, CEO of Anitian, “Building a Multi-Generational Security Program.” Presentation to the Mad Scientist Conference, 14 September 2016.

Bruce Potter, Founder, Shmoo Group; Comments on the Mad Scientist Panel: “Community of Hackers and Makers and Innovative Thinkers”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

SSG Anthony Quill, Comments on the Mad Scientist Panel: “Cyber Talent Management from the Junior Perspective” Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

APPENDIX E: REFERENCES

Dr. David Raymond, Deputy Director, IT Security Lab, Virginia Tech; Comments on the Mad Scientist Panel: “Educating the Cyber Force of 2050”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Franklin S. Reeder and Katrina Timlin, “Recruiting and Retaining Cybersecurity Ninjas”, Center for Strategic & International Studies, October 2016.

Radhika R. Roy, Joe Law, and Rocio Bauer; TNP, CSIA, S&TCD, CERDEC, APG, MD; “Future Army Cyber Security Networking Architecture Framework”, paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.

David E. Sanger, “Countering Cyberattacks Without a Playbook”, New York Times, 23 December 2014.

David E. Sanger, “It’s No Cold War, But Vladimir Putin Relishes His Role As Disrupter.” NY Times 30 Sep 2016.

Jacquelyn Schneider, Digitally-Enabled Warfare: The Capability-Vulnerability Paradox, CNAS Report August 2016.

Brian Schultz and Blade Rhoades, “Strategic Broadening for Mid-Career Cyber Leaders, paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.

George M. Schwartz, Immaculata University, “Developing Cybersecurity Proficiency in an Era of Accelerating Change: Utilizing a Bachelor Degree Foundation for Emerging Professionals”, paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.

SSG Dane Sebring, Comments on the Mad Scientist Panel: “Cyber Talent Management from the Junior Perspective” Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Peter Singer, “How the United States Can Win the Cyber War of the Future,” Foreign Policy, December 8 2015.

LTC Dan Smith, Assistant Professor, USMA; Comments on the Mad Scientist Panel: “Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century”, Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Jessica “Zhanna” Malekos Smith, “Twilight Zone Conflicts: Employing Gray Tactics in Cyber Operations”, Small Wars Journal, October 27, 2016 at http://smallwarsjournal.com/jrnl/art/twilight-zone-conflicts-employing-gray-tactics-in-cyber-operations.

Francesca Spidalieri and Jennifer McArdle, “Transforming the Next Generation of

APPENDIX E: REFERENCES

Military Leaders into Cyber-Strategic Leaders: The Role of Cybersecurity Education in US Service Academies," The Cyber Defense Review (Spring 2016).

James Stavridis. "How to Win the Cyberwar Against Russia". Foreign Policy, October 12, 2016 at http:// foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

CPT Rock Stevens, Comments on the Mad Scientist Panel: "Cyber Talent Management from the Junior Perspective" Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Scott Stevenson, Comments on the Mad Scientist Panel: "Building & Evolving the Right Culture and Workforce to Thrive in the 21st Century", Mad Scientist Conference: the 2050 Cyber Army, 13 September 2016.

Andrew Tilghman, Military Times, "Does Cyber Corps Merit Its Own Service Branch?" Military Times, April 10, 2015.

Joshua Toman, Chambers Clerk; Comments on the Mad Scientist Panel: "Challenges and Opportunities in Partnerships", Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.

Nicholas Ryan Turza, "Counterattacking the Comment Crew: the Constitutionality of Presidential Policy Directive 20 as a Defense to Cyberattacks", North Carolina Journal of Law & Technology 15 N.C. J.L. & TECH. ON. 134 (2014).

United States Army, ARDP 1-02 Terms and Military Symbols.

United States Army Cyber Command, The U.S. Army Landcyber White Paper, 2018-2030, Army Cyber Command (9 September, 2013).

United States Department of Defense, "The DOD Cyber Strategy." Department of Defense, April 17, 2015.

United States Department of Defense, Quadrennial Defense Review, 2014.

United States Joint Staff, Joint Publication 3-12 Cyberspace Operations.

United States of America. The White House. Office of the President. International Strategy for Cyberspace. 16 May 2011.

United States of America, White House Policy Report, "Cyber Defense Deterrence Policy", December 2015.

APPENDIX E: REFERENCES

COL Carlos Vega, Army Cyber Institute; Comments on the Mad Scientist Panel:" Challenges and Opportunities in Partnerships", Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.

Matt Weaver, Rogue Leader, Digital Defense Service; "Pervasive Capability: Our Only Hope", Presentation to the Mad Scientist Conference: the 2050 Cyber Army, 14 September 2016.

Robert Zager and John Zager, "Why We Will Continue to Lose the Cyber War (Response to Cyber Proficient Force 2015 and Beyond)", paper submitted to the Mad Scientist Conference: the 2050 Cyber Army, 2016.