FY18 Mad Scientist Laboratory Anthology

This page intentionally left blank

Table of Contents

Introduction

Welcome to the FY18 Mad Scientist Laboratory Anthology!

This anthology serves as a sample of futures oriented assessments published in the blog over the last year. The assessments include ideas about the future operational environment, technology trends, innovation, and our conference findings. Each article includes a wealth of links to interesting content including Mad Scientist videos, podcasts, conference proceedings, and presentations.

The Mad Scientist Laboratory is an open source, crowdsourced, running estimate of future possibilities and their military implications. There are no facts about the future, but this form of horizon scanning serves to help limit confirmation bias and the bandwagon effect of groupthink with regard to the changing character of future warfare and the convergence of disruptive technologies driving this change.

The Mad Scientist Laboratory published 86 assessments in FY18 with 39 submitted by guest bloggers from academia, industry, our Army Labs, think tanks, and our Sister Services. After reading some of these articles, consider subscribing at: **http://madsciblog.tradoc.army.mil/** and think about authoring our next guest post.

Submit your questions about the Anthology and forward your draft posts to the Mad Scientist group email account: **usarmy.jble.tradoc.mbx.army-mad-scientist@mail.mil**

Further connect to Mad Scientist by following us on Twitter - **@ArmyMadSci**

Return to the Table of Contents

This page intentionally left blank

Chapter 1. The Future Operational Environment

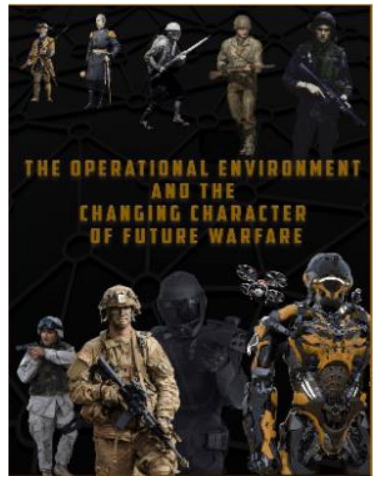
Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 25 (1 FEB 18)

25. Lessons Learned in Assessing the Operational Environment

(**Editor's Note:** The Mad Scientist Laboratory is pleased to present the following guest blog post from **Mr. Ian Sullivan**.)



During the past year, the U.S. Army Training and Doctrine Command (TRADOC) G-2 has learned a great deal more about the Future Operational Environment (OE). While the underlying assessment of the OE's trajectory has not changed, as reported in last year's ***The Operational Environment and the Changing Character of Future Warfare***, we have learned a number of critical lessons and insights that affect Army doctrine, training, and modernization efforts. These findings have been captured in ***Assessing the Operational Environment: What We Learned Over the Past Year***, published in ***Small Wars Journal*** last week. This post extracts and highlights key themes from this article.

General Lessons Learned:

We have confirmed our previous analysis of trends and factors that are intensifying and accelerating the transformation of the OE. The rapid innovation, development, and fielding of new technologies promises to radically enhance our abilities to live, create, think, and prosper. The accelerated pace of human interaction and widespread connectivity through the Internet of Things (IoT), and the concept of convergence are also factors affecting these trends. Convergence of societal trends and technologies will create new capabilities or societal implications that are greater than the sum of their individual parts, and at times are unexpected.

This convergence will embolden global actors to challenge US interests. The perceived waning of US military power in conjunction with the increase in capabilities resulting from our adversaries' rapid proliferation of technology and increased investment in research and development has set the stage for challengers to pursue interests contrary to America's.

We will face peer, near-peer, and regional hegemons as adversaries, as well as non-state actors motivated by identity, ideology, or interest, and individuals super-empowered by technologies and capabilities once found only among nations. They will directly attack our national will with cyber and sophisticated information operations.

Technologies in the future OE will be disruptive, smart, connected, and self-organizing. Key technologies, once thought to be science fiction, present new opportunities for military operations ranging from human operated / machine-assisted, to human-machine hybrid operations, to human-directed / machine-conducted operations; all facilitated by autonomy, Artificial Intelligence (AI), robotics, enhanced human performance, and advanced computing.

Tactical Lessons Learned:

The tactical lessons we have learned reveal tangible realities found on battlefields around the globe today and our assessments about the future rooted in our understanding of the current OE. Our adversaries already are using weapons and systems that in some cases are superior to our own, providing selective overmatch of some US capabilities, such as long-range fires, air-defense, and electronic warfare. **Commercial-off-the shelf (COTS) technologies** are being used to rapidly create new and novel methods of warfare (the most ubiquitous are drones and robotics that have been particularly successful in Iraq, Syria, and Ukraine). Our adversaries will often combine technologies or operating principles to create innovative methods of attack, deploying complex combinations of capabilities that create unique challenges to the Army and Joint Forces.

Adversaries, regardless of their resources, are finding ways to present us with multiple tactical dilemmas. They are combining capabilities with new concepts and doctrine, as evidenced by Russia's New Generation Warfare; China's active defensive and local wars under "informationized" conditions; Iran's focus on information operations, asymmetric warfare and anti-access/area denial; North Korea's combination of conventional, information

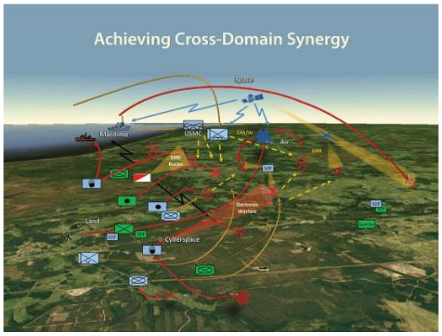
operations, asymmetric, and strategic capabilities; ISIS's often improvised yet complex capabilities employed during the Battle of Mosul, in Syria, and elsewhere; and the proliferation of anti-armor capabilities seen in Yemen, Iraq, and Syria, as well as the use of ballistic missiles by state and non-state actors.

Our adversaries have excelled at **Prototype Warfare**, using new improvised capabilities that converge technologies and COTS systems—in some cases for specific attacks—to great effect. ISIS, for example, has used commercial drones fitted with 40mm grenades to attack US and allied forces near Mosul, Iraq and Raqaa, Syria. While these attacks caused little damage, a Russian drone dropping a thermite grenade caused **the destruction of a Ukrainian arms depot at Balakleya**, which resulted in massive explosions and fires, the evacuation of 23,000 citizens, and $1 billion worth of damage and lost ordnance.

Additionally, our adversaries continue to make strides in developing Chemical, Biological, Radiological, and Nuclear (CBRN) capabilities. We must, at a tactical level, be prepared to operate in a CBRN environment.

Operational Lessons Learned:

Operational lessons learned are teaching us that our traditional—and heretofore very successful—ways of waging warfare will not be enough to ensure victory on future battlefields. Commanders must now sequence battles and engagements beyond the traditional land, sea, and air domains, and seamlessly, and often simultaneously, orchestrate combat effects across multi-domains, to include space and cyberspace. The multiple tactical dilemmas that our adversaries present us with create operational level challenges. Adversaries are building increasingly sophisticated anti-access/area denial “bubbles” we have to break; extending the scope of operations through the use of cyber, space, and asymmetric activities; and are utilizing sophisticated, and often deniable, methods of using information operations, often enabled by cyber capabilities, to directly target the Homeland and impact our individual and national will to fight. This simultaneous targeting of individuals and segments of populations has been addressed in our **Personalized Warfare** post.



We will have to operationalize Multi-Domain Battle to achieve victory over peer or near-peer competitors. Additionally, we must plan and be prepared to integrate other government entities and allies into our operations. The dynamism of the future OE is driven by the ever increasing volumes of information; when coupled with sophisticated whole-of-government approaches, information operations — backed by new capabilities with increasing ranges — challenge our national approach to warfare. The importance of information operations will continue, and may become the primary focus of warfare/competition in the future.

When adversaries have a centralized leadership that can send a unified message and more readily adopt a whole-of-government approach, the US needs mechanisms to more effectively coordinate and collaborate among whole-of-government partners. Operations short of war may require the Department of Defense to subordinate itself to other Agencies, depending on the objective. Our adversaries’ asymmetric strategies blur the lines between war and competition, and operate in a gray zone between war and peace below the perceived threshold of US military reaction.

Strategic Lessons Learned:

Strategic lessons learned demonstrate the OE will be more challenging and dynamic then in the past. A robust Homeland defense strategy will be imperative for competition from now to 2050. North Korea's strategic nuclear capability, if able to range beyond the Pacific theater to CONUS, places a renewed focus on weapons of mass destruction and missile defense. A broader array of nuclear and weapons of mass destruction-armed adversaries will compel us to re-imagine operations in a CBRN environment, and to devise and consider new approaches to deterrence and collective security. Our understanding of deterrence and coercion theory will be different from the lessons of the Cold War.

The Homeland will be an active theater in any future conflict and adversaries will have a host of kinetic and non-kinetic attack options from our home stations all the way to the combat zone. The battlefield of the future will become far more lethal and destructive, and be contested from home station to the Joint Operational Area, requiring ways to sustain operations, and also to rapidly reconstitute combat losses of personnel and equipment. The Army requires resilient **smart installations** capable of not only training, equipping, preparing, and caring for Soldiers, civilians, and families, but also efficiently and capably serving as the first point of power projection and to provide reach back capabilities.

Trends in demographics and climate change mean we will have to operate in areas we might have avoided in the past. These areas include cities and megacities, or whole new theaters, such as the Arctic.

Personalized warfare will increase over time, specifically targeting the brain, genomes, cultural and societal groups, individuals' personal interests/lives, and familial ties.

Future conflicts will be characterized by **AI vs AI** (i.e., algorithm vs algorithm). How AI is structured and integrated will be the strategic advantage, with the decisive edge accruing to the side with more autonomous decision-action concurrency on the "Hyperactive Battlefield." Due to the increasingly interconnected Internet of Everything and the proliferation of weapons with highly destructive capabilities to lower echelons, tactical actions will have strategic implications, putting even more strain and time-truncation on decision-making at all levels. Cognitive biases can shape our actions despite unprecedented access to information.

The future OE presents us with a combination of new technologies and societal changes that will intensify long-standing international rivalries, create new security dynamics, and foster instability as well as opportunities. The Army recognizes the importance of this moment and is engaged in a modernization effort that rivals the intellectual momentum following the 1973 Starry Report and the resultant changes the "big five" (i.e., M1 Abrams Tank, M2 Bradley Fighting Vehicle, AH-64 Apache Attack Helicopter, UH-60 Black Hawk Utility Helicopter, and Patriot Air Defense System) wrought across leadership development and education, concept, and doctrine development that provided the U.S. Army overmatch into the new millennium.

Based on the future OE, the Army's leadership is asking the following important questions:

- What type of force do we need?
    - What capabilities will it require?
        - How will we prepare our Soldiers, civilians, and leaders to operate within this future?

Clearly the OE is the starting point for this entire process.

For additional information regarding the Future OE, please see the following:

Technology and the Future of War podcast, hosted by the ***Modern War Institute*** at the U.S. Military Academy in West Point, New York.

An Advanced Engagement Battlespace: Tactical, Operational and Strategic Implications for the Future Operational Environment, posted on ***Small Wars Journal***.

OEWatch, a monthly on-line, open source journal, published by the TRADOC G-2's Foreign Military Studies Office (FMSO).

Ian Sullivan *is the Assistant G-2, ISR and Futures, at Headquarters, TRADOC.*

Return to the Table of Contents

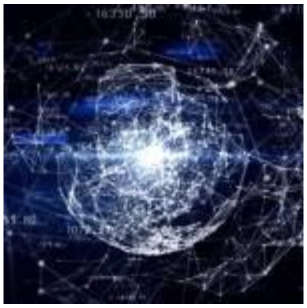
This page intentionally left blank

Mad Scientist Laboratory Blog Post 7 (20 Nov 17)

7. Timeless Competitions

The nature of war remains inherently humanistic and largely unchanging. That said, Mad Scientists must understand the changing character of warfare in the future Operational Environment, as discussed on pages 16-18 of **The Operational Environment and the Changing Character of Future Warfare**. With emergences in technologies that are so significant, extensive, and pervasive, warfare will be transformed – made faster, more destructive, and fought at longer ranges; targeting civilians and military equally across the physical, cognitive, and moral dimensions; and (if waged effectively) securing its objectives before actual battle is joined. Although the character of warfare changes dramatically, there are a number of timeless competitions that will endure for the foreseeable future.

Finders vs Hiders. As in preceding decades, that which can be found, if unprotected, can still be hit. By 2050, it will prove increasingly difficult to stay hidden. Most competitors can access space-based surveillance, networked multi-static radars, a wide variety of drones / swarms of drones, and a vast array of passive and active sensors that are far cheaper to produce than the countermeasures required to defeat them. Quantum computing and advanced sensing will open new levels of situational awareness. Passive sensing, especially when combined with artificial intelligence and big-data techniques, may routinely outperform active sensors. Hiding will still be possible, but will require a dramatic reduction of thermal, electromagnetic, and optical signatures. More successful methods may involve "hiding" amongst an obscuration of emitters and signals – presenting adversaries with a veritable needle within a stack of like-appearing and emitting needles.

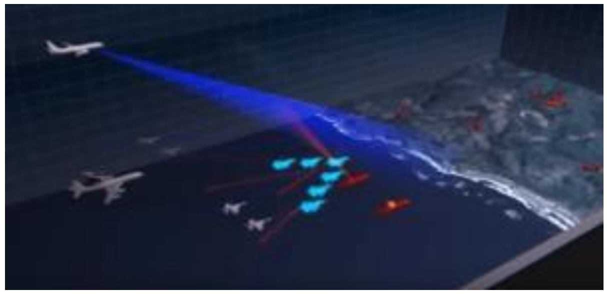


Strikers vs Shielders. Precision strike will improve exponentially through 2050, with the type of precision once formerly reserved for high-end aerospace assets now extended to all domains and at every echelon of engagement. Combatants, both state and non-state, will have a host of advanced delivery options available to them, including advanced kinetic weapons, hypersonics, directed energy (including laser and microwave), and cyber. Space-based assets will become increasingly integrated into striker-shielder complexes, with sensors, anti-satellite weapons, and possibly space-to- earth strike platforms.

At the same time, and on the other end of the spectrum, it will be possible to deploy swarms of massed, low-cost, self-organizing unmanned systems (directed by bio-mimetic algorithms) to overwhelm opponents, offering an alternative to expensive, exquisite systems. With operational range spanning from the strategic – including the homeland – to the tactical, the application of advanced fires from one domain to another will become routine. A wide range of effects can be delivered by a striker, ranging from point precision to area suppression using thermobarics, brilliant cluster munitions, and even a variety of nuclear, chemical, or biological systems. Shielders, on the other hand, will focus on an integrated approach to defense, which target enemy finders, their linkages to strikers, or the strikers themselves.

Protection vs Access. While protection vs. access is generally thought about in physical terms, there is a more prevalent competition emerging in the future regarding cyber protection and access to data. Data is increasingly important, as it underpins AI, machine learning, decision-making, and battlefield management. Due to its vital but often sensitive nature, there is a tension point between the need to access friendly and adversarial information and the need for both sides to protect it.

Planning and Judgement vs Reaction and Autonomy. The mid-Century duel for the initiative has a unique character. New operational tools offer extraordinary speed and reach and often precipitate unintended consequences. Commanders will need to open multi-domain windows through which to deliver effects, balancing deliberate planning to set conditions with "*l'audace*" — the ability to rapidly exploit opportunities and strike at vulnerabilities as they appear — thereby achieving success against sophisticated defensive deployments and shielder complexes.



This will place an absolute imperative on ISR, as well as on intelligence analysis that is augmented by AI, big data, and advanced analytic techniques to determine the conditions on the battlefield, and specifically when, and for how long, a window of operation is open. On the defensive, a commander will be faced with increasingly short decision cycles, with automation and artificial intelligence-assisted decisions becoming the norm. Man-machine teaming will be essential to staff planning, with carefully trained, educated, and possibly cognitive performance-enhanced personnel working to create and exploit opportunities. This means that Armies no longer merely adapt between wars, but do so between and during short-term engagements.

Escalation vs De-Escalation. The competition between violence escalation and de-escalation will be central to stability, deterrence, and strategic success. Violence is readily available on unprecedented scales to a wide-range of actors. Conventional and cyber capabilities can be so potent as to generate effects on the scale of WMD. State and non-state actors alike will utilize hybrid strategies and “Gray Zone” operations, demonstrating a willingness to escalate conflict to a level of violence that exceeds the interests of an adversary to intervene. Long-range strikers and shielder complexes, which extend from the terrestrial domains into space – taken together with cyber technology and more ubiquitous finders – are significantly destabilizing and allow a combatant a freedom of maneuver to achieve objectives short of open war. The ability to effectively escalate and de-escalate along a scalable series of options will be a prominent feature of force design, doctrine, and policy by mid-Century.

These timeless competitions prompt the following questions:

1) What kind of R&D implications might each of these competitions have? Does R&D become increasingly ceded to the private sector as technological advances become exceedingly agnostic to defensive and offensive focuses?

2) In what ways do technological shifts in society impact these timeless competitions? (i.e., does the emergence of the Internet of Things – and eventually Internet of Everything – re-characterize Hiders vs. Finders?)

3) Does the democratization of technology and information increase the role of the Army in land warfare or does the pervasive nature of these technologies and cyber force the Army to incorporate itself more in a whole-of-government approach?

4) What kind of changes do the evolutions of timeless competitions bring about to Army force structuring, organization, strategy, tactics, training, and recruiting?

For further discussions regarding these Timeless Competitions, please see pages 43-49 of the **Robotics, Artificial Intelligence & Autonomy Conference Final Report**, and **An Advanced Engagement Battlespace: Tactical, Operational and Strategic Implications for the Future Operational Environment**

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 52 (14 May 18)

52. Potential Game Changers

The **Mad Scientist Initiative** brings together cutting-edge leaders and thinkers from the technology industry, research laboratories, academia, and across the military and Government to explore the impact of **potentially disruptive technologies**. Much like Johannes Gutenberg's moveable type (illustrated above), these **transformational game changers** have the potential to impact how we live, create, think, and prosper. Understanding their **individual** and **convergent impacts** is essential to continued **battlefield dominance** in the **Future Operational Environment**. In accordance with **The Operational Environment and the Changing Character of Future Warfare**, we have divided this continuum into two distinct timeframes:

The Era of Accelerated Human Progress (Now through 2035):
The period where our adversaries can take advantage of **new technologies, new doctrine,** and **revised strategic concepts** to effectively **challenge U.S. military forces** across multiple domains. **Game changers** during this era include:

• **Robotics:** Forty plus countries develop military robots with some level of autonomy. Impact on society, employment.
Vulnerable: To Cyber/Electromagnetic (EM) disruption, battery life, ethics without man in the loop.
Formats: Unmanned/Autonomous; ground/air vehicles/subsurface/sea systems. Nano-weapons.
Examples: (Air) Hunter/killer Unmanned Aerial Vehicle (UAV) swarms; (Ground) Russian Uran: Recon, ATGMs, SAMs.

• **Artificial Intelligence:** Human-Agent Teaming, where humans and intelligent systems work together to achieve either a physical or mental task. The human and the intelligent system will trade-off cognitive and physical loads in a collaborative fashion.

• **Swarms/Semi Autonomous:** Massed, coordinated, fast, collaborative, small, stand-off. Overwhelm target systems. Mass or disaggregate.

• **Internet of Things (IoT):** Trillions of internet linked items create opportunities and vulnerabilities. Explosive growth in low Size Weight and Power (SWaP) connected devices (Internet of Battlefield Things), especially for sensor applications (situational awareness). Greater than 100 devices per human. Significant end device processing (sensor analytics, sensor to shooter, supply chain management).
Vulnerable: To Cyber/EM/Power disruption. Privacy concerns regarding location and tracking.
Sensor to shooter: Accelerate kill chain, data processing, and decision-making.

• **Space:** Over 50 nations operate in space, increasingly congested and difficult to monitor, endanger Positioning, Navigation, and Timing (PNT)

GPS Jamming/Spoofing: Increasingly sophisticated, used successfully in Ukraine.
Anti Satellite: China has tested two direct ascent anti-satellite missiles.

The Era of Contested Equality (2035 through 2050):

The period marked by **significant breakthroughs** in technology and **convergences** in terms of capabilities, which lead to **significant changes** in the **character of warfare**. During this period, traditional aspects of warfare undergo dramatic, almost revolutionary changes which at the end of this timeframe may even challenge the very nature of warfare itself. **Game changers** during this era include:

• Hyper Velocity Weapons:
Rail Guns (Electrodynamic Kinetic Energy Weapons): Electromagnetic projectile launchers. High velocity/energy and space (Mach 5 or higher). Not powered by explosive.
No Propellant: Easier to store and handle.
Lower Cost Projectiles: Potentially. Extreme G-force requires sturdy payloads.
Limiting factors: Power. Significant IR signature. Materials science.
Hyper Glide Vehicles: Less susceptible to anti-ballistic missile countermeasures.

• Directed Energy Weapons: Signature not visible without technology, must dwell on target. Power requirements currently problematic.
Potential: Tunable, lethal, and non-lethal.
Laser: Directed energy damages intended target. Targets: Counter Aircraft, UAS, Missiles, Projectiles, Sensors, Swarms.
Radio Frequency (RF): Attack targets across the frequency spectrum. Targets: Not just RF; Microwave weapons "cook targets," people, electronics.

• Synthetic Biology: Engineering / modification of biological entities
Increased Crop Yield: Potential to reduce food scarcity.
Weaponization: Potential for micro-targeting, Seek & destroy microbes that can target DNA. Potentially accessible to super-empowered individuals.
Medical Advances: Enhance soldier survivability.
Genetic Modification: Disease resistant, potentially designer babies and super athletes/soldiers.
Synthetic DNA stores digital data. Data can be used for micro-targeting.
CRISPR: Genome editing.

• **Information Environment:** Use IoT and sensors to harness the flow of information for situational understanding and decision-making advantage.

In envisioning **Future Operational Environment possibilities**, the Mad Scientist Initiative employs a number of techniques. We have found **Crowdsourcing** (i.e., the gathering of ideas, thoughts, and concepts from a wide variety of interested individuals assists us in diversifying thoughts and challenging conventional assumptions) to be a particularly effective technique. To that end, we have published our latest, 2-page compendium of **Potential Game Changers** **here** — we would like to **hear your feedback** regarding them. Please let us know your thoughts / observations by **posting them** in this blog post's **Comment** box (found below, in the **Leave a Reply** section). Alternatively, you can also submit them to us **via email** at: usarmy.jble.tradoc.mbx.army-mad-scientist@mail.mil. **Thank you in advance for your contributions!**

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 2 (13 Nov 17)

2. Advanced Engagement Battlespace and the "Hyperactive Battlefield"

Small Wars Journal recently posted a Training and Doctrine Command (TRADOC) assessment entitled "**An Advanced Engagement Battlespace: Tactical, Operational and Strategic Implications for the Future Operational Environment**." Developed in response to a question from the Army Chief of Staff following a Unified Quest (UQ) out brief, it addresses the future character of warfare in the Operational Environment (OE) of 2050, specifically the "Hyperactive Battlefield." The paper's conclusions are drawn from the TRADOC G-2's Mad Scientist Initiative findings and our collaboration with the Army Capabilities Integration Center (ARCIC) and Combined Arms Center (CAC) to explore the idea of Advanced Engagements.

These engagements will be …

… compressed in time, as the speed of weapon delivery and their associated effects accelerate enormously;

… extended in space, in many cases to a global extent, via precision long-range strike and interconnectedness, particularly in the information environment;

… far more lethal, by virtue of ubiquitous sensors, proliferated precision, high kinetic energy weapons and advanced area munitions;

… routinely interconnected – and contested — across the multiple domains of air, land, sea, space and cyber; and

… interactive across the multiple dimensions of conflict, not only across every domain in the physical dimension, but also the cognitive dimension of information operations, and even the moral dimension of belief and values.

The paper discusses a progressively improved Recon / Strike Complex as one of the tactical implications of this "Hyperactive Battlefield":

"The enhanced range, precision and proliferation of Advanced Engagements will render recon / strike effects that are vastly more lethal. Advanced Engagements will also enable a recon / strike complex that is stunningly faster, in many cases collapsing the decision-action cycle to mere milliseconds with automated, human-on-the-loop sensors. AI-enabled visual recognition will identify and classify military targets far faster than humans can. The decisive edge may accrue to the side with more autonomous decision-action concurrency."

"The future recon / strike 'complex,' although extended to more domains, may paradoxically be 'less complex' and redesigned for "disintermediation." Legacy recon / strike complexes depend on a series of orchestrated and carefully constrained intermediary linkages: processes, relationships, and communications architectures designed and optimized for specific combinations of sensors and shooters. A gamechanging capability may accrue to competitors who can design systems that minimize these intermediaries to adroitly link "any sensor / best shooter" combinations on an area basis, regardless of asset ownership, echelon or domain."

The U.S. Army's Force XXI initiative during the waning years of the previous century brought about Digitization and a revolution in what was then called Battle Command.

• What are the ramifications for future Mission (or Conditions) Command required capabilities, given this brave, new Recon / Strike Complex's millisecond decision-action cycles and disintermediation?

Given continuing advances in Artificial Intelligence (AI) and machine learning,

• Can a compelling rationale be made justifying the removal of human judgement from the Observe – Orient – Decide – Act (OODA) loop on the "Hyperactive Battlefield?"

• If so, how do we ensure the continued ethical conduct of war?

• Conversely, is there an ethical rationale compelling the removal of humans from the OODA loop?

Although the authors foresee “paroxysms of intense, hyperactive violence,” they posit combatants quickly transitioning “to a highly leveraged defensive stance” with “defenders … impos[ing] debilitating costs” — leading to protracted campaigns.

• Will this dynamic relegate large maneuver forces to the history books, as the static defenses in depth did to horse cavalry on the Western Front during the Great War?

[Return to the Table of Contents](#)

This page intentionally left blank

Mad Scientist Laboratory Blog Post 48 (26 APR 18)

48. Warfare at the Speed of Thought

(**Editor's Note:** Mad Scientist Laboratory is pleased to present the second guest blog post by **Dr. Richard Nabors**, Associate Director for Strategic Planning and Deputy Director, Operations Division, U.S. Army Research, Development and Engineering Command (RDECOM) Communications-Electronics Research, Development and Engineering Center (CERDEC), addressing how Augmented and Mixed Reality are the critical elements required for integrated sensor systems to become truly operational and support Soldiers' needs in complex environments.

Dr. Nabors' previous guest **post** addressed how the proliferation of sensors, integrated via the Internet of Battlefield Things [IoBT], will provide Future Soldiers with the requisite situational awareness to fight and win in increasingly complex and advanced battlespaces.)

Speed has always been and will be a critical component in **assuring military dominance**. Historically, the military has sought to increase the speed of its jets, ships, tanks, and missiles. However, one of the **greatest leaps** that has yet to come and is coming is the ability to **significantly increase** the **speed** of the **decision-making process** of the individual at the small unit level.

To maximize **individual** and **small unit initiative** to think and act flexibly, **Soldiers** must receive as much **relevant information** as possible, as quickly as possible. **Integrated sensor technologies** can provide **situational awareness** by collecting and sorting real-time data and sending a **fusion of information** to the point of need, but that information must be **processed quickly** in order to be **operationally effective**. **Augmented Reality (AR) and Mixed Reality (MR)** are two of the most promising solutions to this challenge facing the military and will eventually make it possible for Soldiers to **instantaneously respond** to an actively changing environment.

AR and MR function in real-time, bringing the elements of the **digital world** into a Soldier's **perceived real world**, resulting in optimal, timely, and relevant decisions and actions. AR and MR allow for the **overlay** of **information** and **sensor data** into the physical **space** in a way that is intuitive, serves the point of need, and requires minimal training to interpret. AR and MR will enable the U.S. military to **survive** in complex environments by **decentralizing decision-making** from **mission command** and placing substantial capabilities in Soldiers' hands in a manner that **does not overwhelm** them with information.

On a Soldier's display, AR can render **useful battlefield data** in the form of camera imaging and virtual maps, aiding a Soldier's navigation and battlefield perspective. Special indicators can mark people and various objects to warn of potential dangers. Soldier-borne, palm-size **reconnaissance copters** with sensors and video can be directed and tasked instantaneously on the battlefield. Information can be gathered by **unattended ground sensors** and transmitted to a command center, with AR and MR serving as a **networked communication system** between military leaders and the individual Soldier. Used in this way, AR and MR increase Soldier **safety** and **lethality**.

In the **near-term**, the Army Research and Development (R&D) community is investing in the following areas:

• **Reliable position tracking** devices that self-calibrate for head orientation of head-worn sensors.

• Ultralight, ultrabright, ultra-transparent **display eyewear** with wide field of view.

• Three-dimensional viewers with **battlefield terrain visualization**, incorporating real-time data from unmanned aerial vehicles, etc.

In the **mid-term**, R&D activities are focusing on:

• Manned vehicles with sensors and processing capabilities for **moving autonomously**, tasked for **Soldier protection**.

• **Robotic** **assets**, tele-operated, semi-autonomous, or autonomous and imbued with intelligence, with limbs that can **keep pace** with Soldiers and **act as teammates**.

• Robotic systems that contain multiple sensors that respond to **environmental factors** affecting the mission, or have **self-deploying camouflage** capabilities that stay deployed while executing maneuvers.

• Enhanced reconnaissance through **deep-penetration** mapping of building layouts, cyber activity, and subterranean infrastructure.

Once AR and MR prototypes and systems have seen widespread use, the **far term** focus will be on automation that could track and react to a **Soldier's changing situation** by **tailoring** the augmentation the Soldier receives and by coordinating across the unit.

In addition, AR and MR will **revolutionize training**, **empowering Soldiers** to **train as they fight**. Soldiers will be able to use real-time sensor data from unmanned aerial vehicles to **visualize battlefield terrain** with geographic awareness of roads, buildings, and other structures before conducting their missions. They will be able to **rehearse courses of action** and **analyze them** before execution to improve situational awareness.

AR and MR are increasingly valuable aids to **tactical training** in preparation for combat in **complex** and **congested** **environments**.

AR and MR are the critical elements required for integrated sensor systems to become truly operational and support Soldiers' needs in complex environments. Solving the challenge of how and where to use AR and MR will enable the military to get full value from its investments in complex integrated sensor systems.

For more information on how the convergence of technologies will enhance Soldiers on future battlefields, see:

– The discussion on advanced decision-making in ***An Advanced Engagement Battlespace: Tactical, Operational and Strategic Implications for the Future Operational Environment***, published by our colleagues at ***Small Wars Journal***.

– Dr. James Canton's **presentation** from the Mad Scientist Robotics, Artificial Intelligence, & Autonomy Conference at Georgia Tech Research Institute last March.

– Dr. Rob Smith's Mad Scientist Speaker Series presentation on **Operationalizing Big Data**, where he addresses the applicability of AR to sports and games training as an analogy to combat training (noting ***"Serious sport is war minus the shooting"*** — George Orwell).

Dr. Richard Nabors *is Associate Director for Strategic Planning, US Army CERDEC Night Vision and Electronic Sensors Directorate.*

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 5 (22 Nov 17)

5. Personalized Warfare

The future of warfare, much like the future of commerce, will be **personalized**.

Emerging threat capabilities targeting the genome; manipulating individual's personal interests, lives, and familial ties; and subtle coercive / subversive avenues of attack against the human brain will transform war into something far more personalized, scalable, and potentially more attractive to nation-states, non-state actors, and super-empowered individuals.

A recent short dystopian-esque film created by the Future of Life Institute, entitled **Slaughterbots**, highlights the dangers of lethal autonomy in the future but also frames what personalized warfare could look like. Individuals are targeted very precisely by their social media presence and activism against policies deemed important by some government, non-state actor, or even super-empowered individual. While it is not shown in the film, it is possible that machine learning and artificial intelligence are assisting in these targeting and lethal autonomous efforts. The ever more connected nature of personal lives (familial and social connections) and sensitive personal information – Ethnicity, DNA, biometrics, detailed medical and psychological information – through social media, commerce, work, and financial transactions makes these vulnerabilities even more prominent.

Additionally, due to advances in the field of neuro–mapping, attacking, changing, and protecting the brain – individuals can be targeted even more specifically; environments (populated by people) could truly be shaped in ways that were never possible before.

The focus of warfare may shift from being nation-state centered to something more personal that targets specific individuals, their families, ethnic, societal, or interest groups, or defined segments of populations. This raises a number of important questions regarding the future of ethics, rules of engagement, and the scope of warfare:

1) Given the potential for adversaries to target populations based on their genomes, how do civil societies deter, defend, and (as necessary) respond to such attacks?

2) What constitutes an act of war? What happens when gray zone and asymmetric attacks extend to the living room?

3) Does war become increasingly enticing as attacks and effects can be so personalized?

4) Is influencing and changing the brain (through physical methods: bugs and drugs) the same as attacking someone? Does coercion through these capabilities constitute an act of war?

For further learning on the future of neuroscience in warfare, check out Georgetown University's Chief of the Neuroethics Studies Program, Dr. James Giordano's presentation "**Neurotechnology in National Security and Defense**," as well as a **podcast** featuring Dr. Giordano by our partners at ***Modern War Institute***.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 70 (23 July 18)

70. Star Wars 2050

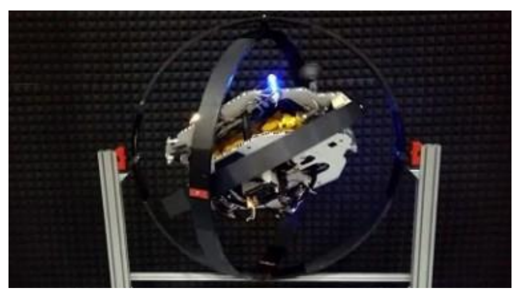
[**Editor's Note:** Mad Scientist Laboratory is pleased to present today's guest post by returning blogger **Ms. Marie Murphy**, addressing the implication of space drones and swarms on space-based services critical to the U.S. Army. Ms. Murphy's previous post addressed **Virtual Nations: An Emerging Supranational Cyber Trend**.]

Drone technology continues to proliferate in militaries and industries around the world. In the deep future, drones and drone swarms may extend physical conflict into the space domain. As space becomes ever more critical to military operations, states will seek technologies to counter their adversaries' capabilities. Drones and swarms can blend in with space debris in order to provide a tactical advantage against vulnerable and expensive assets at a lower cost.

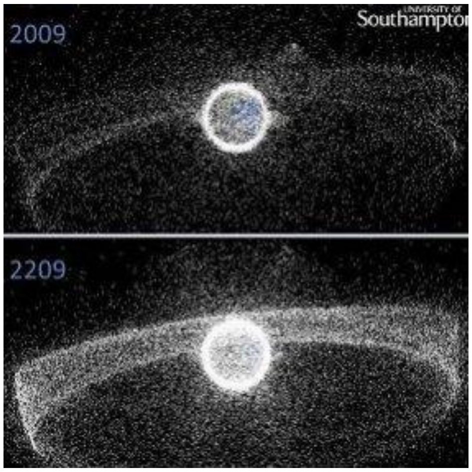
Space was recently identified as a battlespace domain in recognition of threats increasing at an unexpected rate and, in 2013, the **Army Space Training Strategy** was released. The functions of the Army almost entirely depend on space systems for daily and specialized operations, particularly C4ISR and GPS capabilities. "Well over 2,500 pieces of equipment… rely on a **space-based capability**" in any given combat brigade, so an Army contingency plan for the loss of satellite communication is critical.[I] It is essential for the Army, in conjunction with other branches of the military and government agencies, to best shield military assets in space and continue to develop technologies, such as outer space drones and swarms, to remain competitive and secure throughout this domain in the future.

Drone swarms in particular are an attractive military option due to their relative inexpensiveness, autonomy, and durability as a whole. The U.S., China, and Russia are the trifecta of advanced drone and drone swarm technology and also pose the greatest threats in space. In May 2018, Chinese Company CETC launched 200 **autonomous drones**,[II] beating China's own **record** of 119 from 2017.[III] The U.S. has also branched out into swarm technology with the testing of **Perdix** drones, although the U.S. is most known for its use of the high-tech Predator drone.[IV]

Non-state actors also possess rudimentary drone capabilities. In January 2018, Syrian rebels attacked a Russian installation with 13 drones in an attempt to overwhelm Russian defenses. The **Russian military** was able to neutralize the attack by shooting down seven and bringing the remaining six down with electronic countermeasures.[V] While this attack was quelled, it proves that drones are being used by less powerful or economically resourceful actors, making them capable of rendering many traditional defense systems ineffective. It is not a far leap to incorporate autonomous communication between vehicles, capitalizing on the advantages of a fully interactive and cooperative drone swarm.



The same logic applies when considering drones and drone swarms in **space**. However, these vehicles will need to be technologically adapted for space conditions. Potentially most similar to future space drones, the company Swarm Technology launched four nanosats called "**SpaceBees**" with the intention of using them to create a constellation supporting Internet of Things (IoT) networks; however, they did so from India without FCC authorization.[VI] Using nanosats as examples of small, survivable space vehicles, the issues of power and propulsion are the most dominant technological roadblocks. **Batteries** must be small and are subject to failure in extreme environmental conditions and temperatures.[VII] Standard drone **propulsion** mechanisms are not viable in space, where drones will have to rely on cold-gas jets to maneuver.[VIII] Drones and drone swarms can idle in orbit (potentially for weeks or months) until activated, but they may still need hours of power to reach their target. The power systems must also have the ability to direct flight in a specific direction, requiring more energy than simply maintaining orbit.



There is a distinct advantage for drones operating in space: the ability to hide in plain sight among the scattered debris in orbit. Drones can be sent into space on a private or government **launch** hidden within a larger, benign payload.[IX] Once in space, these drones could be released into orbit, where they would blend in with the hundreds of thousands of other small pieces of material. When activated, they would lock onto a target or targets, and swarms would converge autonomously and communicate to avoid obstacles. Threat detection and avoidance systems may not recognize an approaching threat or swarm pattern until it is too late to move an asset out of their path (it takes a few hours for a shuttle and up to 30 hours for the ISS to conduct object avoidance maneuvers). In the deep future, it is likely that there will be a higher number of larger space assets as well as a greater number of nanosats and CubeSats, creating more objects for the **Space Surveillance Network** to track, and more places for drones and swarms to hide.[X]

For outer space drones and drone swarms, the issue of space junk is a double-edged sword. While it camouflages the vehicles, drone and swarm attacks also produce more space junk due to their kinetic nature. One directed "kamikaze" or armed drone can severely damage or destroy a satellite, while swarm technology can be harnessed for use against larger, defended assets or in a coordinated attack. However, projecting shrapnel can hit other military or commercial assets, creating a **Kessler Syndrome** effect of cascading damage.[XI] Once a specific space junk removal program is established by the international community, the resultant debris effects from drone and swarm attacks can be mitigated to preclude collateral damage. However, this reduction of space junk will also result in less concealment, limiting drones' and swarms' ability to loiter in orbit covertly.

Utilizing drone swarms in space may also present legal challenges. The original governing document regarding space activities is the Outer Space Treaty of 1967. This treaty specifically prohibits WMDs in space and the militarization of the moon and other celestial bodies, but is not explicit regarding other forms of militarization, except to emphasize that space activities are to be carried out for the benefit of all countries. So far, military space activities have been limited to deploying military satellites and combatting cyber-attacks. Launching a kinetic attack in space would carry serious global implications and repercussions.

Such drastic and potentially destructive action would most likely stem from intense conflict on Earth. Norms about the usage of space would have to change. The Army must consider how widely experimented with and implemented drone and swarm technologies can be applied to targeting critical and expensive assets in orbit. Our adversaries do not have the same moral and ethical compunctions regarding space applications that the U.S. has as the world's leading democracy. Therefore, the U.S. Army must prepare for such an eventuality. Additionally, the Army must research and develop a more robust alternative to our current space-based GPS capability. For now, the only war in space is the one conducted electronically, but kinetic operations in outer space are a realistic possibility in the deep future.

Marie Murphy *is a rising junior at The College of William and Mary in Virginia, studying International Relations and Arabic. She is currently interning at Headquarters, U.S. Army Training and Doctrine Command (TRADOC) with the Mad Scientist Initiative.*

---

[i] Houck, Caroline, "**The Army's Space Force Has Doubled in Six Years, and Demand Is Still Going Up**," ***Defense One***, 23 August 2017.

[ii] "**China's Drone Swarms**," ***OE Watch***, Vol. 8.7, July 2018.

[iii] "**China Launches Drone Swarm of 11 Fixed-Wing Unmanned Aerial Vehicles**," ***Business Standard***, 11 June 2017.

[iv] Atherton, Kelsey D., "**The Pentagon's New Drone Swarm Heralds a Future of Autonomous War Machines**," ***Popular Science***, 17 January 2017.

[v] Hruska, Joel, "**Think One Military Drone is Bad? Drone Swarms Are Terrifyingly Difficult to Stop**," ***Extreme Tech***, 8 March 2018.

[vi] Harris, Mark, "**Why Did Swarm Launch Its Rogue Satellites?**" **IEEE Spectrum**, 20 March 2018.

[vii] Chow, Eugene K., "**America Is No Match for China's New Space Drones**," **The National Interest**, 4 November 2017.

[viii] Murphy, Mike, "**NASA Is Working on Drones That Can Fly In Space**," ***Quartz***, 31 July 2015.

[ix] Harris, Mark, "**Why Did Swarm Launch Its Rogue Satellites?**" ***IEEE Spectrum***, 20 March 2018.

[x] "**Space Debris and Human Spacecraft**," ***NASA***, 26 September 2013.

[xi] Scoles, Sarah, "**The Space Junk Problem Is About to Get a Whole Lot Gnarlier**," ***WIRED***, July 31, 2017.

Return to the Table of Contents

Chapter 2. Technology Trends

Return to the Table of Contents

This page intentionally left blank

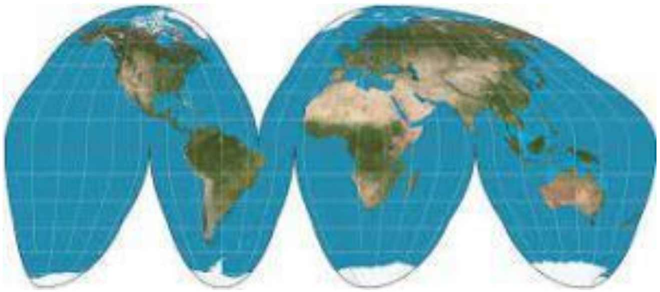
Mad Scientist Laboratory Blog Post 23 (25 Jan 18)

23. Extended Trends Impacting the Future Operational Environment

The Mad Scientist **Strategic Security Environment (SSE) 2050 Conference** 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. Co-sponsored by the TRADOC G-2, the Chief of Staff of the Army's (CSA) Strategic Studies Group (SSG), and Georgetown University's Center for Security Studies, **SSE 2050** informed us that our understanding of the future SSE must first be grounded on what will not change, particularly the enduring nature of war.

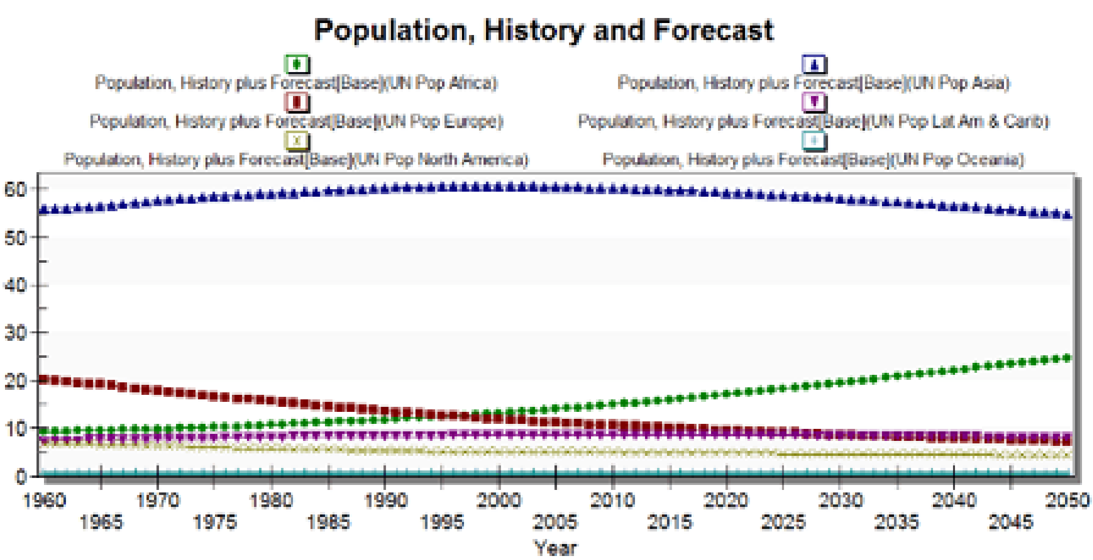
War, intrinsic to the human condition, **will persist as a fundamentally human activity**, and because human nature is in turn enduring, so too is the nature of war. Similarly, the U.S. has enduring interests out to 2050, but we can anticipate an **accelerating collision of interests** as peer competitors assert interests of their own, as do a wider range of threats including Violent Extremist Organizations (VEOs) and super-empowered individuals.

These new warfare approaches leverage a series of extended and emerging trends. **Extended trends** are more readily amenable to long term forecasting; as humans respond to these extended trends, emerging trends become evident — less predictable, to be sure, but nonetheless discernible and significant. The following inexorable demographic and economic changes drive extended trends and are more readily amenable to long term forecasting and projection:



– Geography. Although we tend to view geography as somewhat immutable, even geography will not escape the impact of a global population that will have increased from 2.5 billion in 1950 to 9.5 billion in 2050. Development and climate change will alter even the fundamentals of geography, open arctic sea routes, and raise sea levels at the littorals. Cities will physically cover large areas of the globe with complex urban sprawl and incorporate a global population that will be 66% urbanized. Some megacities will be more important politically and economically than many nation-states; others will out-grow their host state. The convergence of more information, more people, together with less community cohesion, state resources, and governance threaten rampant poverty, violence and pollution: a breeding ground for discontent and anger among an increasingly aware yet still dis-empowered population.

– Demographics. The increase in global population will be far from even: Africa's population will rise, Europe's will decline, as will East Asia, but at a lower rate. European and Asian population average ages will increase while Africa stays young. The disparate growth rates and average ages will drive the direction of migration, unemployment trends, and the availability (and inclination) of individuals fit for military service.



– **Economics.** The distribution of global wealth will become only slightly more equal over the next several decades and this relative improvement will not occur evenly across the globe; the bottom 30% will not see any improvement in their relative economic position. Relative deprivation drives instability; not deprivation per se – and in a world increasingly connected regardless of income level, the deprived will be painfully aware of their relative status.

– **Education.** Education goes up everywhere, but regional differences continue to be significant. The disparate access to quality education will drive uneven economic growth, and differentiate the benefits of participation in global trade.

– **Water Scarcity.** Pollution, contamination, and over-use of many critical water sources will increasingly render water a “non- renewable” resource. Increasing scarcity may drive conflict. Water stress is already high in many portions of the globe, wide-spread water shortages are probable in 2050, with billions potentially impacted.

– Food Scarcity. Certain segments of Africa will see food production significantly lag population growth, though the causes of food scarcity are likely to be domestic conflict, poor governance, and mismanagement rather than a lack of arable land. In 2016, the number of net food importing countries is growing while food price volatility is increasing. This scarcity – together with that of water — will also almost certainly create future migratory pressures and mass population movements, with destabilizing results in both the donor and recipient regions.

– Resource Competition. Growing and shifting populations will increasingly compete for water, food, fossil fuels, and unique mineral resources.

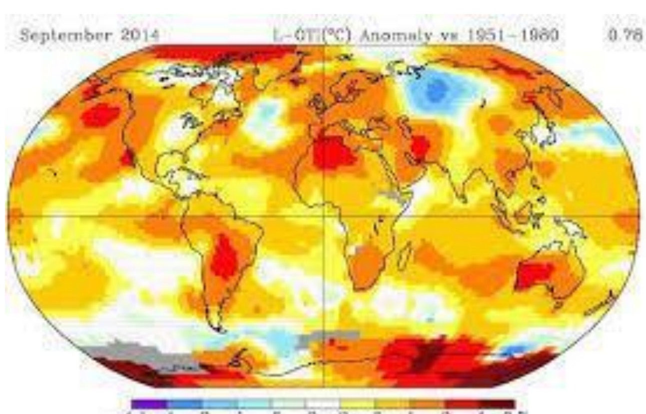
– Mass Migration. The National Intelligence Council predicts that 2030 will be characterized as the "new age of migration." Driven by climate change, water and food scarcity, uneven economic opportunity, and political and social insecurity, mass migration

will pose a significant governance challenge to receiving states as these migrants concentrate predominantly in urban areas. Immigration can result in beneficial, synergistic blending of cultures, ethnicities, and ideologies as groups assimilate into their new region; alternately disparate cultures, ethnic tensions

and stigmatizing stereotypes can force people into small enclaves, pockets and neighborhoods of ethnically homogenous migrants. These isolated areas often suffer from less capable governance including law enforcement, sanitation services, and institutional education opportunities that lag behind most of the host country. The key is the rate at which an immigrant population can be assimilated; if that rate is exceeded, then the impact is destabilizing.

– Energy Demand. Energy demand will continue to rise but extended trends indicate that solutions will keep pace with that demand. Technologies ranging from fracking, fuel cells, controlled (and compact, mobile) nuclear fusion, ocean thermal energy conversions, biomass, and wind provide multiple options to supplement legacy power generation technologies and meet the inevitable rising energy demands of a growing world population. Some of these energy options, however, may exacerbate the extent and rate of climate change. The proliferation of alternative energy sources might suppress fossil fuel costs, impacting major producers whose economic well-being and stability is tied to continued global demand and production.

– Climate Change. Climate change is the great accelerator, exacerbating the impact of water shortages, food insecurity, and even geographic changes.



Our efforts to understand the future strategic security environment illustrate both the enduring nature of war and also the inevitable collision of interests between likely competitors, how our adversaries are adapting, and the extended trends that propel those adaptations. These trends propel our own need to adapt as well, and our understanding cannot be complete without rigorous self-examination.

For information on how these and other trends affect the Operational Environment, see the **OEWatch**, an open source, monthly publication published by the TRADOC G-2's Foreign Military Studies Office (FMSO).

FMSO also publishes a number of OE monographs, some of which address trends identified above, for example: **The Rare Earth Dilemma: Trading OPEC for China**.

Also see Dr. Jonathan D. Moyer's presentation on **Long Term Trends and Some Implications of Decreasing Global Interdependence** from the **SSE 2050** Conference.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 6 (27 Nov 17)

6. Trends in Autonomy

"Control leads to compliance; autonomy leads to engagement." – Daniel H. Pink

During the **Robotics, Artificial Intelligence & Autonomy Conference**, Georgia Tech Research Institute (GTRI), 7-8 March 2017, Mad Scientists addressed how these interdependent technologies will exercise key roles in future military operations, including land operations.

In order to better address Autonomy's relevance to future military operations, the Mad Scientist community identified the following Autonomy Trends:

Autonomy Definition. The Joint Concept for Robotics and Autonomous Systems defines autonomy as follows:

"… the level of independence that humans grant a system to execute a given task. It is the condition or quality of being self-governing to achieve an assigned task based on the system's own situational awareness (integrated sensing, perceiving, analyzing), planning and decision-making. Autonomy refers to a spectrum of automation in which independent decision-making can be tailored for a specific mission, level of risk, and degree of human-machine teaming."

Degrees of Autonomy. The phrase “spectrum of automation” alludes to the different degrees to autonomy:

• **Fully Autonomous:** “Human Out of the Loop”: no ability for human to intervene in real time.

• **Supervised Autonomous:** “Human on the Loop”: humans can intervene in real time.

• **Semi-Autonomous:** “Human in the Loop”: machines wait for human input before taking action.

• **Non-Autonomous (Remote Control):** “Human in the Loop”: machines guided via remote controls; no autonomy in system.

Autonomy Baseline. Autonomy is already evident on the battlefield. At least 30 countries have defensive, human-supervised autonomous weapons such as the Aegis and Patriot. Some “fully autonomous” weapon systems are also emerging. The Israeli Harpy drone (anti-radiation loitering munition) has been sold to India, Turkey, South Korea, and China. China reportedly has reverse-engineered their own variant. The U.S. has also experimented with similar systems in the Tacit Rainbow and the Low Cost Autonomous Attack System (LOCAAS) programs.

Autonomy Projections. Mad Scientists expect autonomy to evolve into solutions that are flexible, multi-modal, and goal-oriented featuring trusted man-machine collaboration, distributed autonomy and continuous learning.

• **Collaborative Autonomy** will be learning and adaptation to perform a new task based on mere demonstration of the task by end-users (i.e., Soldiers) to teach the robot what to do.

• **Distributed Autonomy** will be dynamic team formation from heterogeneous platforms to include coordination in settings with limited or impaired communication and the emergence of new tactics and strategies enabled by multi-agent capabilities.

• **Continuous Learning** will be a continuous, incremental evolution and expansion of capabilities, to include the incorporation of high-level guidance (such as human instruction, changes in laws / ROEs / constraints) and "Transfer Learning."

Autonomy Challenges. Mad Scientists acknowledged that the aforementioned "autonomy projections" pose the following challenges:

• **Goal-Oriented Autonomy:** Decision and adaptation, to include the incorporation of ethics and morality into decision-making.

• **Trusted Collaboration:** The challenge of trust between man and machine continues to be a dominant theme. Machines must properly perceive human goals and preserve their autonomous system integrity while achieving joint man-machine goals in a manner explainable to – and completely trusted by — the human component.

• **Distributed Systems:** Rethinking the execution of tasks using multiple, distributed agents while preserving command-level understanding and decision adds an additional layer of complexity to the already challenging task of designing and building autonomous systems.

• **Transfer Learning:** Learning by inference from similar tasks must address the challenges of seamless adaptation to changing contexts and environments, including the contextual inference of missing data and physical attributes.

• **High Reliability Theory:** "Normal Accident Theory" holds that accidents are inevitable in complex, tightly-coupled systems. "High Reliability Theory" asserts that organizations can contribute significantly to the prevention of accidents. Because of the significant complexity and “tight-coupling” of future autonomous systems, there is an obvious challenge in the application of high reliability theory to emerging technologies that are not yet well comprehended.

Relevance of Autonomous Systems. Hollywood inevitably envisions autonomous systems as either predisposed for malevolence, destined to “go rogue” and turn on their creators at the earliest opportunity; or coolly logical, dispassionately taking actions with disastrously unintended consequences for humankind. For the foreseeable future, however, no autonomous system will have the breadth, robustness and flexibility of human cognition. That said, autonomous systems offer the potential for speed, mass, and penetration capabilities in future lethal, high threat environments — minimizing risks to our Soldiers.

For additional insights regarding Autonomy Trends, watch “**Unmanned and Autonomous Systems**,” presented by Mr. Paul Scharre, Senior Fellow / Director, Future Warfare Initiative, Center for New American Security, during the GTRI Conference last spring.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 11 (14 Dec 17)

11. Artificial Intelligence (AI) Trends

"By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it." – Eliezer Yudkowsky

Few technological advances remain more misunderstood than the potential impact Artificial Intelligence (AI) will have on all aspects of society in the coming years.

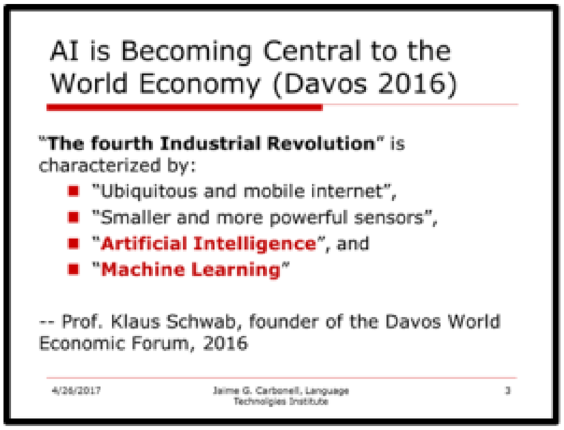
Hollywood and professional prophets of doom share much of the blame in contributing to our confusion and negative biases regarding the coming AI revolution. During the Robotics, Artificial Intelligence & Autonomy Conference, facilitated at Georgia Tech Research Institute (GTRI), 7-8 March 2017, Mad Scientists addressed how AI will play a key role in future military operations. To dispel misconceptions and facilitate a better understanding of AI's relevance to future military operations, Mad Scientist presents the following AI Trends:

AI Definition. Richard Potember of the Mitre Corporation offers the following definition:

"[AI is] conventionally, if loosely, defined as intelligence exhibited by machines. Operationally, it can be defined as those areas of R&D practiced by computer scientists who identify with one or more of the following academic sub-disciplines: Computer Vision, Natural Language Processing (NLP), Robotics (including Human-Robot Interactions), Search and Planning, Multi-agent Systems, Social Media Analysis (including Crowdsourcing), and Knowledge Representation and Reasoning (KRR). The field of Machine Learning (ML) is a foundational basis for AI."

Mad Scientists cited numerous key components to the field of AI, including:
- **Automated Perception** using a range of modalities: vision, sonar, lidar, haptics;
- **Robotic Action** such as locomotion and manipulation;
- **Deep Reasoning:** planning, goal-oriented behavior, projection;
- **Language Technologies:** language, speech, dialog, social nets;
- **Big Data:** storage, processing, analytics and inference;
- **Machine Learning** to include adaptation, reflection, knowledge acquisition.

Mad Scientists treated AI and Cognitive Computing as interchangeable terms.



AI Baseline. Physical robots are merely one type of AI entity. Others include cyber agents, decision aids, the internet of things, and increasingly munitions and networks. Mad Scientists described AI as a key component of the "Fourth Industrial Revolution."

Currently there is a $153B market for AI-enabled technology — with an estimated annual creative disruption impact of $14-33 trillion.

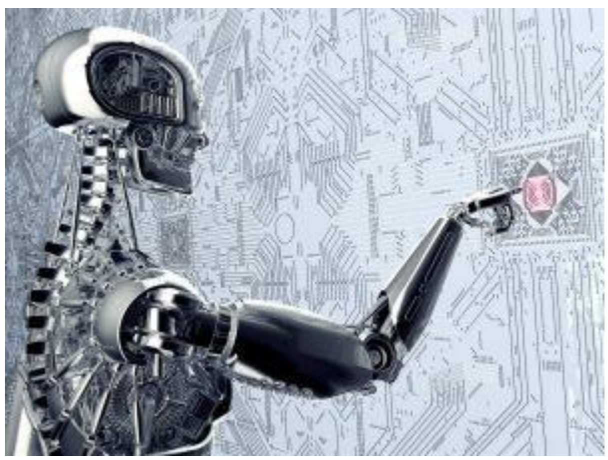
- AI technology is currently advancing at breakneck speeds, with recent interesting accomplishments in a broad range of areas to include:
- Unsupervised learning, generative modeling;
- "Deep Learning" exploiting Deep Neural Networks (DNNs) to facilitate automated interpretation of vision and speech (Neural Language Processing);
- Reinforcement learning for decision-making and robotics "training";
- Multi-task networks, transfer learning;
- Use of simulated data;
- Large-margin methods (SVM) for entity classification; and
- Graphical models.

AI Projections. AI touches virtually every area of computer science and, in the words of one Mad Scientist:

"Everything that we formerly electrified, we will now 'cognitize' — no more 'dumb data.'"

Large sections of the global economy will be run by AI, with widespread disruption to the electrical infrastructure, healthcare, additive manufacturing, transportation sector, supply chain management, and farming. This disruption is not confined to “blue-collar” labor markets; it is also advancing in “white-collar” fields such as financing and equity trading.

Autonomy and learning are already pervasive in sensing, but will increasingly take over decision-making as well. Mad Scientists project future AI capable of reflection, curiosity, and teamwork. AI may extend language translation capabilities, perhaps even to other species. Individuals may eventually exercise ubiquitous personalized agents (i.e., “Cogs”), and artificial intelligence will extend the boundary of “self.” **Human judgment will remain essential, but the line of decision allocation between humans and machines will be shifting in coming years**.



AI Challenges.

• **Maturity.** Current AI systems are frequently “brittle” (i.e., narrow applications that can generate “very dumb” results when operated outside of narrow constraints). They are also vulnerable to spoofing.

• **Big Data and Active Learning.** Big Data is the fuel that drives deep learning, and is “big” not only from a quantity perspective. It is also “big” from the perspective of a high level of complexity (potential relations among entries) and dimensionality (attributes per entry).

Paradoxically, Big Data is often associated with “Knowledge Sparsity” because only a tiny fraction of the vast amounts of Big Data is effectively labeled. Less than .01% of all galaxies in the Sloan Sky Survey have consensus labels; less than .0001% of all web pages have topic labels. Less than .0001% of all financial transactions are investigated and labeled as fraudulent / non-fraudulent. Mad Scientists described “Active Learning” as a potential technique to address knowledge sparsity by teaming AI capabilities with external assistance that selects the portions of Big Data with maximum potential impact on learning.

• **DoD Problem Set.** Mad Scientists acknowledge that there are unique characteristics of the DoD space including a lack of data, more complex sensing phenomena, the high risk of deception, the requirement for multi-source fusion and distributed sensing, and the significant consequences of military decision-making. Current DoD acquisition processes, moreover, cannot keep pace with the transformative rate of change in the AI field.

• **Explainability.** The complexity of AI systems is a double-edged sword, wherein enhanced capability is paradoxically paired with decreased explainability. The nature of machine learning – particularly machine learning based on deep neural networks — is such that we often don’t understand exactly how it works. The way such systems are currently designed, moreover, such understanding is not possible. This is at the heart of “trust” issues between the man-machine team.

Therefore several Mad Scientists projected a future dichotomy between “Safe AI” and “AI in the Wild.” Safe AI might come with guarantees, constraints, transparency, and a “universal ‘undo’ button.” “Wild AI” would approach full autonomy with unrestricted adaptability, curiosity, and exploration – and no ironclad guarantees. Artificial General Intelligence (AGI) might fit into this latter category and be a potential game-changer of existential proportion.

Relevance of AI Systems. AI can both reinforce and mitigate the accelerating scope and pace of warfare, integrating decision making across domains and enabling sub-millisecond decisions. Expertise is perishable and doesn’t scale: enhanced decision making AI can restore balance to the Observe, Orient, Decide, Act (OODA) loop; complementing past investments in “Observe” and “Assessment” with improved focus on “Orientation” and “Deciding.” AI

“Battle Buddies” may enhance a Soldier’s personal Situational Awareness through proactive intelligence gathering and analysis; ultimately having the potential to drive the downsizing of staffs and mobile headquarters. Training can be enhanced through virtual / augmented realties.

AI may facilitate the visualization of combat effects in the cyber domain through augmented reality. Some challenges, particularly data challenges, have such magnitude that adequate numbers of people can simply not be mustered to address them. AI will be essential in such instances.

For additional insights regarding AI Trends, watch “Artificial Intelligence and Machine Learning: Potential Application in Defense Today and Tomorrow,” presented by Mr. Louis Maziotta, Armament Research, Development, and Engineering Center (ARDEC), during the GTRI Conference last spring.

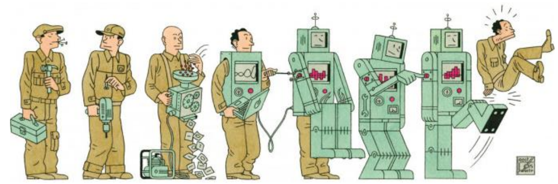
Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 56 (29 May 18)

56. An Appropriate Level of Trust…

The **Mad Scientist team** participates in many thought **exercises, tabletops,** and **wargames** associated with how we will **live, work,** and **fight in the future**. A **consistent theme** in these events is the idea that a **major barrier** to the **integration** of robotic systems into Army formations is **a lack of trust** between humans and machines. This assumption rings true as we hear the **media** and **opinion polls** describe how **society doesn't trust** some **disruptive technologies**, like driverless cars or the **robots coming for our jobs**.



In his recent book, Army of None, **Paul Scharre** describes an **event** that nearly led to a **nuclear confrontation** between the **Soviet Union** and the **United States**. On September 26, 1983, **LTC Stanislav Petrov**, a **Soviet Officer** serving in a bunker outside Moscow was **alerted** to a **U.S. missile launch** by a **recently deployed space-based early warning system**. The Soviet Officer trusted his "gut" – or **experientially informed intuition** – that this was a **false alarm**. His gut was right and the **world was saved** from an **inadvertent nuclear exchange** because this officer **did not over trust** the system. But is this **the rule** or **an exception** to how humans **interact with technology?**

The **subject of trust** between **Soldiers, Soldiers and Leaders,** and the **Army and society** is **central** to the idea of the **Army as a profession**. At the most **tactical level**, **trust is** seen as **essential** to **combat readiness** as Soldiers must trust each other in dangerous situations. Humans naturally learn to **trust their peers** and **subordinates** once they have worked with them for a period of time. You learn **what** someone's **strengths and weaknesses** are, **what** they can **handle**, and under **what conditions** they will struggle. This human dynamic **does not translate** to **human-machine interaction** and the tendency to **anthropomorphize machines** could be a huge barrier.

We recommend that the Army **explore the possibility** that **Soldiers** and **Leaders** could **over trust AI** and **robotic systems**. **Over trust** of these systems could **blunt human expertise, judgement,** and **intuition** thought to be **critical** to winning in **complex operational environments**. Also, over trust might lead to **additional adversarial vulnerabilities** such as **deception** and **spoofing.**

In 2016, a research team at the **Georgia Institute of Technology** revealed the results of a study entitled "**Overtrust of Robots in Emergency Evacuation Scenarios**". The research team put 42 test participants into a **fire emergency** with a **robot** responsible for **escorting them to an emergency exit**. As the robot **passed obvious exits** and **got lost**, 37 participants continued to follow the **robot** and an additional 2 **stood with the robot** and **didn't move towards either exit**. The study's takeaway was that **roboticists** must think about programs that will **help humans** establish an **"appropriate level of trust"** with **robot teammates**.

In [Future Crimes](), **Marc Goodman** writes of the idea of "**In Screen We Trust**" and the **vulnerabilities** this **trust builds** into our **interaction** with our **automation**. His example of the cyber-attack against the Iranian uranium enrichment centrifuges **highlights** the **vulnerability** of **experts believing** or **trusting their screens** against **mounting evidence** that something else might be contributing to the failure of centrifuges. These experts **over trusted** their technology or just did not have an "**appropriate level of trust**". What does this have to do with **Soldiers** on the **future battlefield**? Well, increasingly we **depend** on our **screens** and, in the future, our **heads-up displays** to translate the world around us. This translation will only **become more demanding** on the future battlefield with **war at machine speed**.

So what should our **assumptions** be about **trust** and our **robotic teammates** on the **future battlefield**?

1) Soldiers and Leaders will **react differently** to **technology integration**.

2) **Capability developers** must account for **trust building factors** in physical **design**, natural **language processing**, and **voice communication**.

3) **Intuition** and **judgement** remain a **critical** component of **human-machine teaming** and operating on the future battlefield. **Speed** becomes a **major challenge** as **humans** become the **weak link**.

4) Building an "**appropriate level of trust**" will need to be part of **Leader Development** and **training**. **Mere expertise** in a field **does not prevent over trust** when **interacting** with our **robotic teammates**.

5) Lastly, **lack of trust** is **not a barrier** to **AI** and **robotic integration** on the **future battlefield**. These **capabilities** will exist in our formations as well as those of our **adversaries**. The formation that develops the **best concepts** for effective **human-machine teaming,** with **trust** being a **major component,** will have the **advantage**.

Interested in learning more on this topic? Watch Dr. Kimberly Jackson Ryan (Draper Labs).

[**Editor's Note:** A special word of thanks goes out to fellow Mad Scientist **Mr. Paul Scharre** for sharing his ideas with the Mad Scientist team regarding this topic.]

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 55 (24 May 18)

55. Influence at Machine Speed: The Coming of AI-Powered Propaganda

[**Editor's Note:** Mad Scientist Laboratory is pleased to present the following guest blog post by **MAJ Chris Telley**, U.S. Army, assigned to the Naval Postgraduate School, addressing how **Artificial Intelligence (AI)** must be understood as an **Information Operations (IO)** tool if U.S. defense professionals are to develop **effective countermeasures** and **ensure our resilience** to its employment by potential adversaries.]

AI-enabled IO present a more pressing **strategic threat** than the **physical hazards** of slaughter-bots or even **algorithmically-escalated** nuclear war. IO are efforts to "**influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries**;" here, we're talking about using AI to do so. **AI-guided IO tools** can empathize with an audience to say anything, in any way needed, to **change** the **perceptions** that drive those physical weapons. **Future IO systems** will be able to individually **monitor** and **affect** tens of thousands of people at once. Defense professionals must understand the **fundamental influence potential** of these technologies if they are to drive security institutions to **counter malign AI use** in the information environment.

Programmatic marketing, using consumer's data habits to drive real time automated bidding on personalized advertising, has been used for a few years now. **Cambridge Analytica**'s Facebook targeting made international headlines using similar techniques, but digital electioneering is just the tip of the iceberg. An AI trained with data from users' social media accounts, economic media interactions (Uber, Applepay, etc.), and their devices' positional data can **infer predictive knowledge** of its targets. With that knowledge, emerging tools — like Replika — can truly befriend a person, allowing it to **train** that individual, for good or ill.

Substantive feedback is required to **train** an **individual's response**; humans tend to **respond best** to **content** and **feedback** with which they **agree**. That content can be **algorithmically mass produced**. For years, Narrative Science tools have helped writers create sports stories and stock summaries, but it's just as easy to use them to **create disinformation**. That's just text, though; today, the **AI** can create **fake video**. A recent warning, ostensibly from former President Obama, provides an entertaining yet frightening demonstration of how Deepfakes will challenge our **presumptions about truth** in the coming years. The **Defense Advanced Research Projects Agency (DARPA)** is funding a project this summer to determine whether **AI-generated Deepfakes** will become impossible to distinguish from the real thing, even using other AI systems.

Given that **malign actors** can now employ **AI** to **lie** "at machine speed," they still have to get the story to an audience. **Russian** bot armies continue to make headlines doing this very thing. The **New York Times** maintains about a dozen Twitter feeds and produces **around 300 tweets a day**, but **Russia's Internet Research Agency (IRA)** regularly puts out 25,000 tweets in the **same twenty-four hours**. The **IRA's bots** are really just **low-tech curators**; they **collect, interpret,** and **display** desired information to **promote** the **Kremlin's narratives**.

Next-generation bot armies will employ far faster computing techniques and profit from an order of magnitude greater network speed when 5G services are fielded. If "**Repetition is a key tenet of** IO execution," then this **machine gun-like** ability to **fire information** at an audience will, with **empathetic precision** and **custom content**, provide the means to change a decisive audience's **very reality**. No breakthrough science is needed, no bureaucratic project office required. These pieces are already there, waiting for an **adversary** to put them together.

The DoD is looking at AI but remains focused on image classification and swarming quadcopters while **ignoring** the **convergent possibilities** of **predictive audience understanding, tailored content production,** and **massive scale dissemination.** What little digital IO we've done, sometimes called social media "**WebOps**," has been **contractor heavy** and **prone** to **naïve missteps**. However, groups like USSOCOM's SOFWERX and the students at the **Naval Postgraduate School** are advancing the state of our art. At NPS, future senior leaders are working on AI, now. A half-dozen of the school's departments have stood up **classes** and events specifically aimed at **operationalizing advanced computing**. The young defense professionals currently working on AI should grapple with **emerging influence tools** and form the **foundation** of the DoD's **future institutional capabilities**.

MAJ Chris Telley *is an Army information operations officer assigned to the Naval Postgraduate School. His assignments have included theater engagement at U.S. Army Japan and advanced technology integration with the U.S. Air Force. Chris commanded in Afghanistan and served in Iraq as a United States Marine. He tweets at @chris_telley.*

This blog post represents the opinions of the author and do not reflect the position of the Army or the United States Government.

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 14 (26 Dec 17)

14. Robotic Trends

Karel Čapek, an early Twentieth Century Czech playwright, coined the expression "Robot" in his 1921 play entitled, "R.U.R" (i.e., "Rossum's Universal Robots"). According to Professor Howard Markel, University of Michigan:

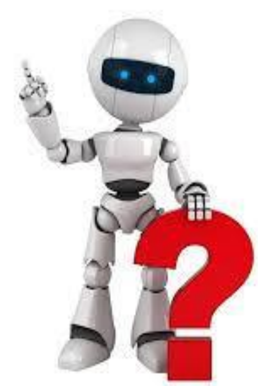
The word Robot *"… comes from an Old Church Slavonic word, rabota, which means servitude of forced labor…. it's really a product of [the] Central European system of serfdom, where a tenants' rent was paid for in forced labor or service."* – from Professor Markel's radio interview with Mr. Ira Flatow, Science Friday, on National Public Radio, 22 April 2011.

This popular play (penned three years following the Armistice ending The Great War and four years after the Bolshevik Revolution birthed the Soviet Union), ignited our collective, dystopian view of robots with a tale of rebellion and the subsequent extinction of mankind.

Flash forward a century to the Robotics, Artificial Intelligence & Autonomy Conference, facilitated at Georgia Tech Research Institute (GTRI), 7-8 March 2017, where Mad Scientists shed a more optimistic light on the role of Robotics in the future – our findings are captured in the following paragraphs:

Robotics Definition. The Joint Staff Concept for Robotics and Autonomous Systems (JCRAS) defines robotics as …

"… powered machines capable of executing a set of actions by direct human control, computer control, or a combination of both. They are comprised minimally of a platform, software, and a power source."



The JCRAS goes on to note that *"Robotic and Autonomous Systems (RAS) is an accepted term in academia and the science and technology (S&T) community; it highlights the physical (robotic) and cognitive (autonomous) aspects of these systems. For purposes of the JCRAS concept, RAS is a* *framework to describe systems with a robotic element, an autonomous element, or more commonly, both. As technology advances, there will be more robotic systems with autonomous capabilities as well as non-robotic autonomous systems."*

Robotics, particularly advanced robotics, typically leverage both Artificial Intelligence (AI) and autonomy and are the physical manifestation by which we experience these trends in our daily lives.

There is a taxonomy for Robotic Systems that includes the following ranges of control:

• **Remote Control.** A mode of operation wherein the human operator, without benefit of video or other sensory feedback, directly controls the actuators of an Un-Manned System (UMS) on a continuous basis, from off the vehicle and via a tethered or radio linked control device using visual line of sight cues. In this mode, the UMS takes no initiative and relies on continuous or nearly continuous input from the user.

• **Augmented Teleoperation.** A mode of operation wherein the human operator leverages video or other sensory feedback to directly control the actuators of a UMS on a continuous basis.

• **Semi-Autonomy.** The condition or quality of being partially self-governing to achieve an assigned mission based on the system's pre-planned situational awareness (integrated sensing, perceiving, analyzing) planning and decision-making. This independence is a point on a spectrum that can be tailored to the specific mission, level of acceptable risk, and degree of human-machine teaming.

• **Full Autonomy.** Full independence that humans grant a system to execute a given task in a given environment.

Robotics Baseline. DOD has already experienced an “Accidental Robot Evolution,” with thousands of air and ground robots developed, deployed, and employed in Iraq and Afghanistan. Up to now, the default perception has been robots as caged “stupid machines” to do routine and dangerous work. Increasingly, however, robots are coming “out of the cages” and migrating into our daily lives.

Robotics Projection. Mad Scientists project a future that features ever more advanced human-robot collaboration, a collaboration that in turn will accelerate the development of improved robotics through rapid machine learning, adaptive controls, rapid algorithm development, and custom motion control systems.

Novel mechanisms and high performance actuators will emerge as new construction paradigms merge component design to generate compact multi-function systems that are both highly capable and energy efficient. Human-robotic system interaction will include conversational assistants, intent and emotion recognition, augmented reality, self-aware explainable systems, and multi-modal communications.

Robotics are already beginning to transform production capabilities; this process will accelerate as collaborative robotic autonomy enables robotic learning and adaptation by simple demonstration. Although a typical current production line today features only 1 product per line, changeover cycles of 2 weeks, and a part cycle time of 6 seconds; future robotics-enabled production will be a flexible configuration of 10+ products per line, nearly zero time required for changeover, 6 second cycle times and sub-millimeter precision.

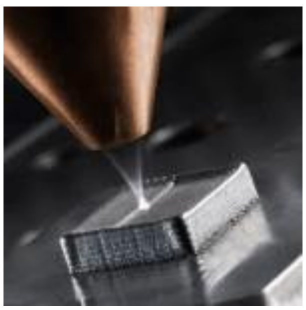
One Mad Scientist asserted a future for "Self-Organizing Matter" in the 2030-2050 timeframe, a future where almost every object will have some degree of self-assembly and self-configuring capability, as the migration of robotics into our everyday experiences advances, robotic appearances may change. It is not likely that they will evolve to be ever more human in appearance, because humanoid shapes are sub-optimal for many jobs or tasks. Robotic forms can be tailored to the task rather than the other way around. Future robotics will be less immediately recognizable as "robots" and our human terrain will morph to accommodate optimal robotic physical configurations.

One such promising field of research is "soft" robotics – replicating living organic musculature's ability to reach out and grasp objects delicately, using a folding origami structure.

I started working with origami many years ago because I was interested in making modular robots that have programmable properties; I wanted to create programmable matter…. We've shown a combination of four muscles that forms an arm with a gripper that can pick up a tire…. If we put a joint there and added another arm, which is quite easily done, we would be able to not just lift up the tire, but move it and place it anywhere." – excerpt from interview with Professor Daniela Rus, Director, MIT CSAIL, posted in *The Verge*, 27 November 2017.

Robotics Challenges:

• **One to Many Control.** Current robotic controls must extend from singular entities to control of multi-robot systems: formations vice individual interaction. How do we address individual control of truly large robotic teams?



• **Additive Metallic Manufacturing.** To date the application of robotic 3D additive manufacturing has focused on the use of resins and polymers to inexpensively generate shapes and applications amenable to those materials. 3D printing of metal parts requires relatively large and expensive machines, very high-powered lasers and expensive technicians, although there are efforts underway to extend the desktop 3D printing approach to metal manufacturing. Solving the 3D metallic manufacturing problem would truly revolutionize manufacturing.

• **High Expectations.** Humans will expect high reliability performance from robotic systems: 'death by robotic accident' will be unacceptable, even for instances where more frequent death by human accident is already tolerated for non-robotic systems.

• **Cognitive Trades.** Robotics generate risk reduction and performance enhancements, but trade the best cognitive computer available: the human brain. This trade can be mitigated by "Centaur Warfighting": human-machine teaming that is not only possible but in many cases preferable. Hybrid human-machine cognitive architectures may be able to leverage the precision and reliability of automation without sacrificing the robustness and flexibility of human intelligence.

• **Destructive Disruption.** One should also note the potential disruptive impact of the robotics revolution, not only with respect to warfare but across the entire global economy, particularly through the displacement of a substantial portion of the labor force. The debate on the extent of that disruption – and whether this disruption is beneficial or detrimental – remains undecided. Some have argued that technology has always created more jobs than it has destroyed. They claim "Robots Will Save the Economy" and cite robotics as necessary for further improvements in productivity across a wide range of labor-intensive tasks.

Others believe that the extent of the robotics revolution is so fast and so radical that it will exceed the capacity of the labor force to adapt. It is safe to assert that the robotics revolution will challenge even the most adaptive societies and that those less adaptive may experience significant destabilization.

Relevance of Robotic Systems. Robotic systems mitigate the risk of combat while providing significant performance advantages such as speed, efficiency, and resilience. Robotic sensor applications, for example, might include precision sensor positioning, sensor placement in adverse environments, and multiple, distributed sensors and platforms. Just as robotics may advance manufacturing to the next "industrial renaissance," they may also enable transformative efficiencies in the transportation and sustainment of land forces.

For more on Robotics, see Remarks by Dr. Robert Sadowski, U.S. Army Chief Roboticist, and The Network is the Robot by Dr. Alexander Kott, Chief, Network Science Division, Computational and Information Sciences Directorate, U.S. Army Research Laboratory, both of which were presented at the GTRI conference this past spring.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 38 (22 Mar 18)

38. The Multi-Domain "Dragoon" Squad: A Hyper-enabled Combat System

"Victory in the future requires a force consisting of the many, small and smart. The United States and its Joint Force needs to get there first, and when it does, it needs to be aware of any advantages—and limitations—these new capabilities will provide." — Mr. Jeff Becker, from his article entitled, **"How to Beat Russia and China on the Battlefield: Military Robots,"** originally published in The National Interest on 18 March 2018.

In 2016, General Mark Milley, Chief of Staff of the Army, asked if the Army of the future would have divisions and brigades, or whether it would utilize small, elite Special Forces-like units with operational and strategic level capabilities. At the U.S. Army Annual Meeting and Exposition, General Milley stated, ***"I suspect that the organizations and weapons and doctrines of land armies, between 2025 and 2050, in that quarter-century period of time, will be fundamentally different than what we see today."*** There is a need to change, **perhaps radically**, some of our organizational unit designs that will allow the Army to operate on the battlefield of the future, which will be dispersed and dangerous across all domains.

To mitigate and disrupt the threat from state and non-state actors with **drastically improved reconnaissance** – persistent Intelligence, Surveillance, and Reconnaissance (ISR), electronic detection capabilities, and a saturation of sensors – and **extremely lethal strike capabilities** – thermobarics, penetrators, dual warheads, hypersonic weapons, long-range artillery, strike and interdiction aircraft – the U.S. Army must consider how to assemble and combine advanced capabilities into **technologically-superior land units** able to attack and destroy larger enemy units, maneuver over the land domain, and seize and hold terrain in support of these missions. Additionally, these forces must have **organic**, or at least more readily available, **cyber, space, and information warfare capabilities**.

The need for these land forces to **operate in and across multiple domains** prompted General Milley to order the creation of an experimental combat unit known as the **Multi-Domain Task Force**. The Army recognizes that future combat units will have to be moderately **self-sustaining, highly lethal, very fast,** and **very difficult to pin down on a battlefield**; current Army force structure does not provide units that can maneuver and operate in this vein. The Multi-Domain Task Force will be the **test bed** for a **concept of operations and force structure** that moves beyond just countering adversarial anti-access and area denial (A2/AD) capabilities and will **incorporate larger Joint efforts for maneuver and combat operations in the future.**

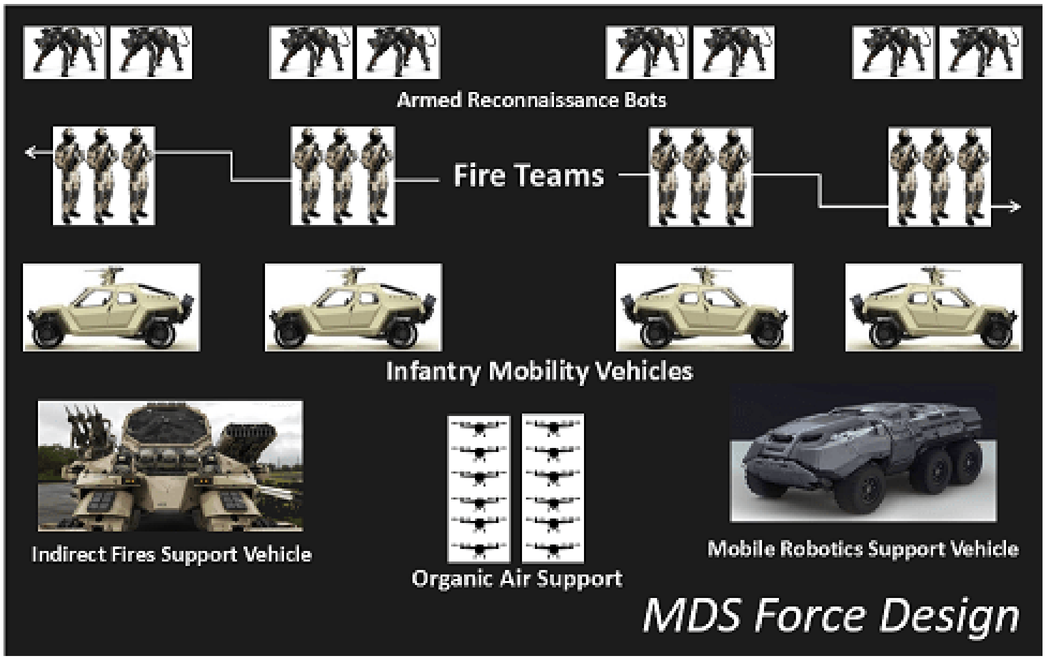
Beyond the challenges and opportunities for operational forces more equivalent to today's brigade combat teams, there is growing concern over the **loss of technological and mobility overmatches** the Army has possessed for the last 15 years at the tactical level.

To explore this problem, **Mr. Jeff Becker**, President and Principal Analyst of Context LLC (and Mad Scientist Laboratory guest blogger), spoke at the Mad Scientist Visualizing Multi Domain Battle Conference at Georgetown University, 25-26 July 2017, about what the **tactical system** of the Army might look like in the **2035-2050 timeframe**. In his video presentation from this conference, Mr. Becker addressed just how **lethal**, how **mobile**, how **protected,** and how **aware** a very small – 12-15 person – unit on the future battlefield might be. He presented the concept for a **Multi-Domain "Dragoon" Squad (MDS)**, a hyper-enabled combat system composed of numerous future technologies allowing the tactical unit to have **multi-domain effects**.

The MDS provides the Army with a small unit capable of **tactical surprise** and an enormous capability for **close-in lethality**. The crux of the MDS is a **system-of-systems approach** to enabling a small tactical unit with the capability to survive, thrive, and bring about **effects across domains throughout the tactical environment in a terrain-agnostic way.**

Multi-Domain Dragoon Squad Composition

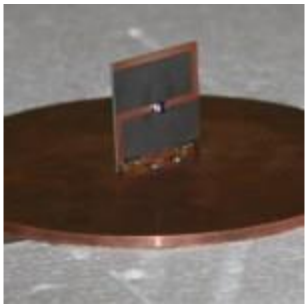
- 12x soldiers, organized in four fire teams
- 4x Infantry Mobility Vehicles (IMVs)
- 8x Armed Reconnaissance Robots (Quadrupedal "Cheetah" variant)
- 1x Autonomous Mobile Robotics Support Vehicle (MRS-V)
- 1x Autonomous Indirect Fires Support Vehicle (IFS-V)



This approach is achieved through multiple technological implementations:

– Equipping of soldiers with soft **"**exosuits**"** to increase their strength and endurance, allowing for heavier and more capable individual weaponry and the ability to **sustain peak performance**

– Lightweight **helmet-mounted displays** providing **augmented** and **virtual reality** images based on feeds from sensors – including cyber and electromagnetic environments to reach **new levels of close-in** situational awareness



– **Metamaterials** allowing lower profile, **higher bandwidth antennas** integral to the soldier suit as well as the vehicles and robots

– **Modernized assault weapons** including guided rounds, increasing the probability of a hit

– Lightweight (4500 lbs.) **Infantry Mobility Vehicles (IMVs)** capable of semi-autonomy, autonomy, or remote-control as well as the ability to provide covering **fire** with a robotic turret and **precision indirect fires** weapons

– **Sensor system** and associated AI capable of detecting, locating, classifying and prioritizing multiple targets, while providing early warning to fire team

– Eight **armed reconnaissance** robots able to move over ground at speeds in excess of 40-50 miles per hour; capable of **traversing complex terrain quickly** and closing with areas of interest at high speed; potential for lethal capability

– Short range, low altitude **quadcopter drones** providing optical and electronic sensing to the unit, **providing constant updates** to the **AR/VR backbone**; potential for lethal capability

– **Squad Indirect Fires Support Vehicle (SIF-V)** providing a range of **indirect fires directly to each team**

The MDS is not the all-encompassing zenith of the MDB concept but rather is a machination of it at the tactical level that could have a ground-up cumulative change effect. It is impossible for the Army, nor any of its sister services, to completely transform within a decade; however, **sweeping organizational experimentation** and **reconfiguration of existing formations** through initiatives such as the **Multi-Domain Task Force** can lead to such a **transformation**.

Mr. Jeff Becker's vision for the MDS was originally submitted in response to a Mad Scientist Call for Ideas that was subsequently published here by ***Small Wars Journal***.

Mr. Becker and MG David Fastabend (USA-Ret.) co-authored a paper that was the baseline and inspiration for The Operational Environment and the Changing Character of Future Warfare on behalf of the TRADOC G-2.

Mr. Becker and MG Fastabend were also key analytical contributors to the Robotics, Artificial Intelligence & Autonomy: Visioning Multi-Domain Warfare in 2030-2050 Final Report that documented the results of the associated Mad Scientist Conference, co-hosted by Georgia Tech Research Institute, on 7-8 March 2017.

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 63 (25 June 18)

63. Russian Ground Battlefield Robots: A Candid Evaluation and Ways Forward

[**Editor's Note:** We are pleased to present Mad Scientist **Sam Bendett**'s informative guest blog post on the ramifications of current Russian Unmanned Ground Vehicle (UGV) trials in Syria for future autonomous combat systems on the battlefield. Please note that many of Mr. Bendett's embedded links in the post below are best accessed using non-DoD networks.]

Russia, like many other nations, is investing in the development of various unmanned military systems. The Russian defense establishment sees such systems as mission multipliers, highlighting two major advantages: saving soldiers' lives and making military missions more effective. In this context, Russian developments are similar to those taking place around the world. Various militaries are fielding unmanned systems for surveillance, intelligence, logistics, or attack missions to make their forces or campaigns more effective. In fact, the Russian military has been successfully using Unmanned Aerial Vehicles (UAVs) in training and combat since 2013. It has used them with great effect in Syria, where these UAVs flew more mission hours than manned aircraft in various Intelligence, Surveillance, and Reconnaissance (ISR) roles.

Russia is also busy designing and testing many unmanned maritime and ground vehicles for various missions with diverse payloads. To underscore the significance of this emerging technology for the nation's armed forces, **Russian Defense Minister Sergei Shoigu** recently stated that the serial production of ground combat robots for the military "may start already this year."

But before we see swarms of ground combat robots with red stars emblazoned on them, the Russian military will put these weapons through rigorous testing in order to determine if they can correspond to battlefield realities. Russian military manufacturers and contractors are not that different from their American counterparts in sometimes talking up the capabilities of their creations, seeking to create the demand for their newest achievement before there is proof that such technology can stand up to harsh battlefield conditions.

It is for this reason that the Russian Ministry of Defense (MOD) finally established several centers such as Main Research and Testing Center of Robotics, tasked with working alongside the defense-industrial sector to create unmanned military technology standards and better communicate warfighters' needs. The MOD is also running conferences such as the annual "**Robotization of the Armed Forces**" that bring together military and industry decision-makers for a better dialogue on the development, growth, and evolution of the nation's unmanned military systems.

This brings us to one of the more interesting developments in Russian UGVs. Then **Russian Deputy Defense Minister Borisov** recently confirmed that the **Uran-9 combat UGV** was tested in Syria, which would be the first time this much-discussed system was put into combat. This particular UGV is supposed to operate in teams of three or four and is armed with a 30mm cannon and 7.62 mm machine guns, along with a variety of other weapons.

Just as importantly, it was designed to operate at a distance of up to three kilometers (3000 meters or about two miles) from its operator — a range that could be extended up to six kilometers for a team of these UGVs. This range is absolutely crucial for these machines, which must be operated remotely. Russian designers are developing operational electronics capable of rendering the Uran-9 more autonomous, thereby moving the operators to a safer distance from actual combat engagement. The size of a small tank, the Uran-9 impressed the international military community when first unveiled and it was definitely designed to survive battlefield realities….

However, just as “no plan survives first contact with the enemy,” the Uran-9, though built to withstand punishment, came up short in its first trial run in Syria. In a candid admission, **Andrei P. Anisimov**, Senior Research Officer at the 3rd Central Research Institute of the Ministry of Defense, reported on the Uran-9’s critical combat deficiencies during the 10th All-Russian Scientific Conference entitled “***Actual Problems of Defense and Security***,” held in April 2018. In particular, the following issues came to light during testing:

• Instead of its intended range of several kilometers, the Uran-9 could only be operated at distance of “300-500 meters among low-rise buildings,” wiping out up to nine-tenths of its total operational range.

• There were “17 cases of short-term (up to one minute) and two cases of long-term (up to 1.5 hours) loss of Uran-9 control” recorded, which rendered this UGV practically useless on the battlefield.

• The UGV’s running gear had problems – there were issues with supporting and guiding rollers, as well as suspension springs.

• The electro-optic stations allowed for reconnaissance and identification of potential targets at a range of no more than two kilometers.

• The OCH-4 optical system did not allow for adequate detection of adversary’s optical and targeting devices and created multiple interferences in the test range’s ground and airspace.

• Unstable operation of the UGV’s 30mm automatic cannon was recorded, with firing delays and failures. Moreover, the UGV could fire only when stationary, which basically wiped out its very purpose of combat “vehicle.”

• The Uran-9’s combat, ISR, and targeting weapons and mechanisms were also not stabilized.

On one hand, these many failures are a sign that this much–discussed and much-advertised machine is in need of significant upgrades, testing, and perhaps even a redesign before it gets put into another combat situation. The Russian military did say that it tested nearly 200 types of weapons in Syria, so putting the Uran-9 through its combat paces was a logical step in the long development of this particular UGV. If the Syrian trial was the first of its kind for this UGV, such significant technical glitches would not be surprising.

However, the MOD has been testing this Uran-9 for a while now, showing videos of this machine at a testing range, presumably in Russia. The truly unexpected issue arising during operations in Syria had to do with the failure of the Uran-9 to effectively engage targets with its cannon while in motion (along with a number of other issues). Still, perhaps many observers bought into the idea that this vehicle would perform as built – tracks, weapons, and all. A closer examination of the publicly-released testing video probably foretold some of the Syrian glitches – in this particular one, Uran-9 is shown firing its machine guns while moving, but its cannon was fired only when the vehicle was stationary. Another interesting aspect that is significant in hindsight is that the testing range in the video was a relatively open space – a large field with a few obstacles around, not the kind of complex terrain, dense urban environment encountered in Syria. While today's and future battlefields will range greatly from open spaces to megacities, a vehicle like the Uran-9 would probably be expected to perform in all conditions. Unless, of course, Syrian tests would effectively limit its use in future combat.

On another hand, so many failures at once point to much larger issues with the Russian development of combat UGVs, issues that Anisimov also discussed during his presentation. He highlighted the following technological aspects that are ubiquitous worldwide at this point in the global development of similar unmanned systems:

• Low level of current UGV autonomy;

• Low level of automation of command and control processes of UGV management, including repairs and maintenance;

• Low communication range, and;

• Problems associated with "friend or foe" target identification.

Judging from the Uran-9's Syrian test, Anisimov made the following key conclusions which point to the potential trajectory of Russian combat UGV development – assuming that other unmanned systems may have similar issues when placed in a simulated (or real) combat environment:

• These types of UGVs are equipped with a variety of cameras and sensors — and since the operator is presumably located a safe distance from combat, he may have problems understanding, processing, and effectively responding to what is taking place with this UGV in real-time.

• For the next 10-15 years, unmanned military systems will be unable to effectively take part in combat, with Russians proposing to use them in storming stationary and well-defended targets (effectively giving such combat UGVs a kamikaze role).

• One-time and preferably stationary use of these UGVs would be more effective, with maintenance and repair crews close by.

• These UGVs should be used with other military formations in order to target and destroy fortified and firing enemy positions — but never on their own, since their breakdown would negatively impact the military mission.

The presentation proposed that some of the above-mentioned problems could be overcome by domestic developments in the following UGV technology and equipment areas:

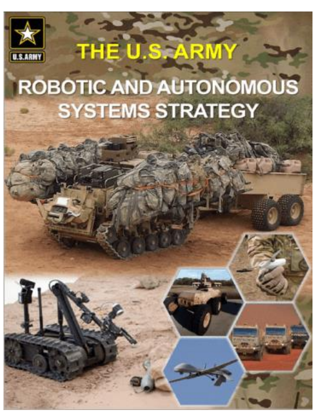
• Creating secure communication channels;

• Building miniaturized hi-tech navigation systems with a high degree of autonomy, capable of operating with a loss of satellite navigation systems;

• Developing miniaturized and effective ISR components;

• Integrating automated command and control systems, and;

• Better optics, electronics and data processing systems.



According to Anisimov's report, the overall Russian UGV and unmanned military systems development arch is similar to the one proposed by the United States Army Capabilities Integration Center (ARCIC): the gradual development of systems capable of more autonomy on the battlefield, leading to "smart" robots capable of forming "mobile networks" and operating in swarm configurations. Such systems should be "multifunctional" and capable of being integrated into existing armed forces formations for various combat missions, as well as operate autonomously when needed. Finally, each military robot should be able to function within existing and future military technology and systems.

Such a candid review and critique of the Uran-9 in Syria, if true, may point to the Russian Ministry of Defense’s attitude towards its domestic manufacturers. The potential combat effectiveness of this UGV was advertised for the past two years, but its actual performance fell far short of expectations. It is a sign for developers of other Russian unmanned ground vehicles – like **Soratnik**, **Vihr**, and **Nerehta** — since it displays full range of deficiencies that take place outside of well-managed testing ranges where such vehicles are currently undergoing evaluation. It also brought to light significant problems with ISR equipment — this type of technology is absolutely crucial to any unmanned system’s successful deployment, and its failures during Uran-9 tests exposed a serious combat weakness.

It is also a useful lesson for many other designers of domestic combat UGVs who are seeking to introduce similar systems into existing order of battle. It appears that the Uran-9’s full effectiveness can only be determined at a much later time if it can perform its mission autonomously in the rapidly-changing and complex battlefield environment. Fully autonomous operation so far eludes its Russian developers, who are nonetheless still working towards achieving such operational goals for their combat UGVs. Moreover, Russian deliberations on using their existing combat UGV platforms in one-time attack mode against fortified adversary positions or firing points, tracking closely with ways that Western military analysts are thinking that such weapons could be used in combat.

The Uran-9 is still a test bed and much has to take place before it could be successfully integrated into current Russian concept of operations. We could expect more eye-opening “lessons learned” from its’ and other UGVs potential deployment in combat. Given the rapid proliferation of unmanned and autonomous technology, we are already in the midst of a new arms race. Many states are now designing, building, exporting, or importing various technologies for their military and security forces.

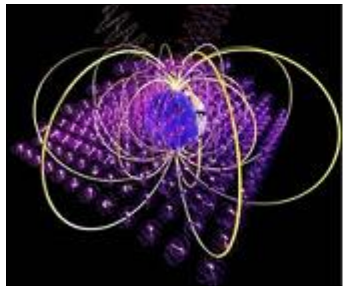
To make matters more interesting, the Russians have been public with both their statements about new technology being tested and evaluated, and with possible use of such weapons in current and future conflicts. There should be no strategic or tactical surprise when military robotics are finally encountered in future combat.

Samuel Bendett *is a Research Analyst at the CNA Corporation and a Russia Studies Fellow at the American Foreign Policy Council. He is an official Mad Scientist, having presented and been so proclaimed at a previous Mad Scientist Conference. The views expressed here are his own.*

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 84 (20 Sep 18)



84. Quantum Surprise on the Battlefield?

[**Editor's Note:** In the following guest blog post, Mad Scientist **Elsa B. Kania** addresses quantum technology and the potential ramifications should the People's Republic of China (PRC) win the current race in fielding operational quantum capabilities].

If China were to succeed in realizing the full potential of quantum technology, the Chinese People's Liberation Army (PLA) might have the capability to offset core pillars of U.S. military power on the future battlefield. Let's imagine the worst-case (or, for China, best-case) scenarios.

The Chinese military and government could leverage quantum cryptography and communications to enable "perfect security" for its most sensitive information and communications. The PLA may look to employ 'uncrackable' quantum key distribution (QKD), which involves the provably secure exchange of keys in quantum states, over fiber optic networks for secure command and control, while extending the range of its quantum networks to more far-flung units or even ships at sea, through an expanding constellation of quantum satellites.

If China were to 'go dark' to U.S. intelligence capabilities as a result, then a new level of uncertainty could complicate U.S. calculus and assessments, while exacerbating the risks of surprise or misperception in a crisis or conflict scenario.

China's massive investments in quantum computing could succeed someday in the decadal marathon towards a fully functional and universal quantum computer.

If developed in secret or operational sooner than expected, then these immense computing capabilities could be unleashed to break public key cryptography. Such asymmetric cryptography, which today is quite prevalent and integral to the security of our information technology ecosystem, relies upon the difficulty of prime factorization, a task beyond the capabilities of today's classical computers but that could be cracked by a future quantum computer. The impact could be analogous to the advantage that the U.S. achieved through the efforts of American code-breakers ahead of the Battle of Midway.

Although there will be options available for 'quantum-proof' encryption, the use of public key cryptography could remain prevalent in older military and government information systems, such as legacy satellites. Moreover, any data previously collected while encrypted could be rapidly decrypted and exploited, exposing perhaps decades of sensitive information. Will the U.S. military and government take this potential security threat seriously enough to start the transition to quantum-resistant alternatives?

Future advances in quantum computing could be game changers for intelligence and information processing. In a new era in which data is a critical resource, the ability to process it rapidly is at a premium. In theory, quantum computing could also accelerate the development of artificial intelligence towards a closer approximation to "superintelligence," provoking concerns of unexpected, by some accounts even existential, risks and powerful capabilities.

Meanwhile, based on active efforts in the Chinese defense industry, the next generation of Chinese submarines could be equipped with a 'quantum compass' to enable greater precision in positioning and independence from space-based navigation systems, while perhaps also leveraging quantum communications underwater for secure control and covert coordination.

The PLA might realize its ambitions to develop quantum radar that could be the "nemesis" of U.S. stealth fighters and bolster Chinese missile defense. This "offset" technology could overcome the U.S. military's advantage in stealth. Similarly, the 'spooky' sensitivity in detection enabled by techniques such as ghost imaging and quantum remote sensing could enhance PLA ISR capabilities.

In the aggregate, could China's future advances in these technologies change the balance of power in the Indo-Pacific?

For China, the potential to disrupt paradigms of information dominance through quantum computing and cryptography, while perhaps undermining U.S. advantages in stealth technologies through quantum radar and sensing, and even more actively contesting the undersea domain, could create a serious challenge to U.S. military-technological predominance.

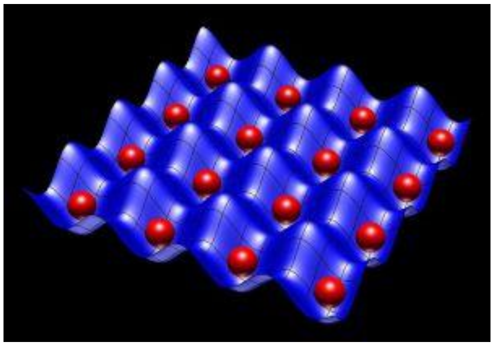
Perhaps, but this imagining of impactful military applications of quantum technology is far from a reality today. For the time being, these technologies still confront major constraints and limitations in their development.

It seems unlikely that quantum cryptography will ever enable truly perfect security, given the perhaps inevitable human and engineering challenges, along with remaining vulnerabilities to exploitation.

At present, quantum computing, while approaching the symbolic milestone of "quantum supremacy," faces a long road ahead, due to challenges of scaling and error correction.

Certain quantum devices, for sensing, metrology, and positioning, may be quite useful but could enable fairly incremental, evolutionary improvements relative to the full range of alternatives.

There are also reasons to consider critically when Chinese official media discloses (especially in English) oft-hyped advances such as in quantum radar – since reporting on such apparent progress could be variously intended for purposes of signaling or perhaps even misdirection.



Although China's advances and ambitions should be taken quite seriously – particularly considering the talent and resources evidently mobilized to advance these objectives – the U.S. military may also be well postured to leverage quantum technology on the future battlefield.

Inevitably, the timeframe for the actual operationalization of these technologies is challenging to evaluate, especially because a significant proportion of the relevant research may be occurring in secret.

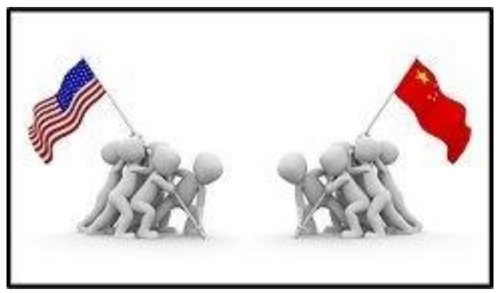
For that reason, it is also difficult to determine with confidence whether the U.S. or China is truly leading in the advancement of various disciplines of quantum science.

Moreover, beyond concerns of competition between the U.S. and China, exciting research is occurring worldwide, from Canada and Europe to Australia, often with tech companies and start-ups at the forefront of the development and commercialization of these technologies.

Looking forward, the trajectory of this second quantum revolution will play out over decades to come. Future successes will require sustained investments, such as those China is actively pursuing in the range of tens of billions.

As the Chinese military and defense industry start testing and experimenting with quantum technology, the U.S. military should also explore further the potential – and evaluate the limitations – of these capabilities, including through deepening public-private partnership.

As China challenges American leadership in innovation, the U.S. military and government should recognize the real risks of future surprises that could result from truly 'made in China' innovation, while also taking full advantage of the opportunities to impose surprise upon strategic competitors.



The above blog post is based on the recently published ***Center for a New American Security (CNAS)*** report entitled *Quantum Hegemony? – China's Ambitions and the Challenges to U.S. Innovation Leadership*, co-authored by **Ms. Elsa Kania** and Mr**. John Costello**. Mad Scientist believes that this report is the best primer on the current state of quantum technology. Note that quantum science – communication, computing, and sensing – was previously addressed by the Mad Scientist Laboratory as a *Pink Flamingo*.

Ms. Kania was proclaimed an official Mad Scientist following her presentation on *PLA Human-Machine Integration* at the ***Bio Convergence and Soldier 2050 Conference*** at SRI International, Menlo Park, 8-9 March 2018. Her podcast from this event, China's Quest for Enhanced Military Technology, is hosted by ***Modern War Institute***.

Ms. Kania *is an Adjunct Fellow with the Technology and National Security Program at CNAS.*
Disclaimer: The views expressed in this article belong to the author alone and do not represent the Department of Defense, the U.S. Army, or the U.S. Army Training and Training Doctrine Command.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 22 (22 Jan 18)

22. Speed, Scope, and Convergence Trends

"Speed is the essence of war. Take advantage of the enemy's unpreparedness; travel by unexpected routes and strike him where he has taken no precautions." — Sun Tzu

This timeless observation from The Art of War resonates through the millennia and is of particular significance to the Future Operational Environment

Mad Scientist Laboratory has addressed the impact of Autonomy, Artificial Intelligence (AI), and Robotic Trends in previous posts. Consequential in their own right, particularly in the hands of our adversaries, the impact of these technology trends is exacerbated by their collective **speed**, **scope**, and **convergence**, leading ultimately to man-machine **co-evolution**.

Speed. Some Mad Scientists posit that the rate of progress in these technologies will be "faster than Moore's law." As our adversaries close the technology gap and potentially overtake us in select areas, there is clearly a "need for speed" as cited in the Defense Science Board (DSB) Report on Autonomy. The speed of actions and decisions will need to increase at a much higher pace over time.

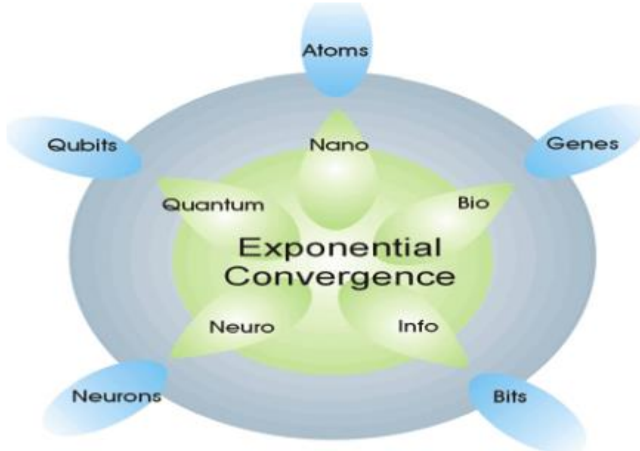
"… the study concluded that autonomy will deliver substantial operational value across an increasingly diverse array of DoD missions, but the DoD must move more rapidly to realize this value. Allies and adversaries alike also have access to rapid technological advances occurring globally. In short, speed matters—in two distinct dimensions. First, autonomy can increase decision speed, enabling the U.S. to act inside an adversary's operations cycle. Secondly, ongoing rapid transition of autonomy into warfighting capabilities is vital if the U.S. is to sustain military advantage." — DSB Summer Study on Autonomy, June 2016 (p. 3)

Scope. It may be necessary to increase not only the pace but also the scope of these decisions if these technologies generate the ***"extreme future"*** characterized by Mad Scientist Dr. James Canton as ***"hacking life" / "hacking matter" / "hacking the planet."*** In short, no aspect of our current existence will remain untouched. Robotics, artificial intelligence, and autonomy – far from narrow topics – are closely linked to a broad range of enabling / adjunct technologies identified by Mad Scientists, to include:

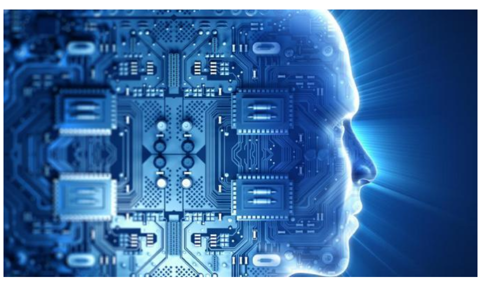
• Computer Science, particularly algorithm design and software engineering
• Man-Machine Interface, to include Language / Speech and Vision
• Sensing Technologies
• Power and Energy
• Mobility and Manipulation
• Material Science to include revolutionary new materials
• Quantum Science
• Communications
• 3D (Additive) Manufacturing
• Positioning, Navigation and Timing beyond GPS
• Cyber

Science and Technological Convergence. Although 90% of the technology development will occur in the very fragmented, uncontrolled private sector, there is still a need to view robotics, artificial intelligence and autonomy as a holistic, seamless system. Technology convergence is a recurring theme among Mad Scientists. They project that we will alter our fundamental thinking about science because of the "exponential convergence" of key technologies, including:

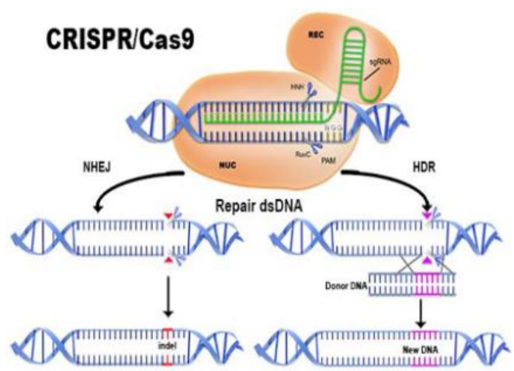
• Nanoscience and nanotechnology
• Biotechnology and Biomedicine
• Information Technology
• Cognitive Science and Neuroscience
• Quantum Science



This convergence of technologies is already leading to revolutionary achievements with respect to sensing, data acquisition and retrieval, and computer processing hardware. These advances in turn enable machine learning to include reinforcement learning and artificial intelligence. They also facilitate advances in hardware and materials, 3D printing, robotics and autonomy, and open-sourced and reproducible computer code. Exponential convergence will generate “extremely complex futures” that include capability “building blocks” that afford strategic advantage to those who recognize and leverage them.



Co-Evolution. Clearly humans and these technologies are destined to co-evolve. Humans will be augmented in many ways: physically, via exoskeletons; perceptionally, via direct sensor inputs; genetically, via AI-enabled gene-editing technologies such as CRISPR; and cognitively via AI “COGs” and “Cogni-ceuticals.” Human reality will be a “blended” one in which physical and digital environments, media and interactions are woven together in a seamless integration of the virtual and the physical. As daunting – and worrisome – as these technological developments might seem, there will be an equally daunting challenge in the co-evolution between man and machine: **the co-evolution of trust**.



Trusted man-machine collaboration will require validation of system competence, a process that will take our legacy test and verification procedures far beyond their current limitations. Humans will expect autonomy to be nonetheless “directable,” and will expect autonomous systems to be able to explain the logic for their behavior, regardless of the complexity of the deep neural networks that motivate it. These technologies in turn must be able to adapt to user abilities and preferences, and attain some level of human awareness (e.g., cognitive, physiological, emotional state, situational knowledge, intent recognition).

For additional information on **The Convergence of Future Technology**, see Dr. Canton's presentation from the Mad Scientist **Robotics, Artificial Intelligence, & Autonomy Conference** at Georgia Tech Research Institute last March.

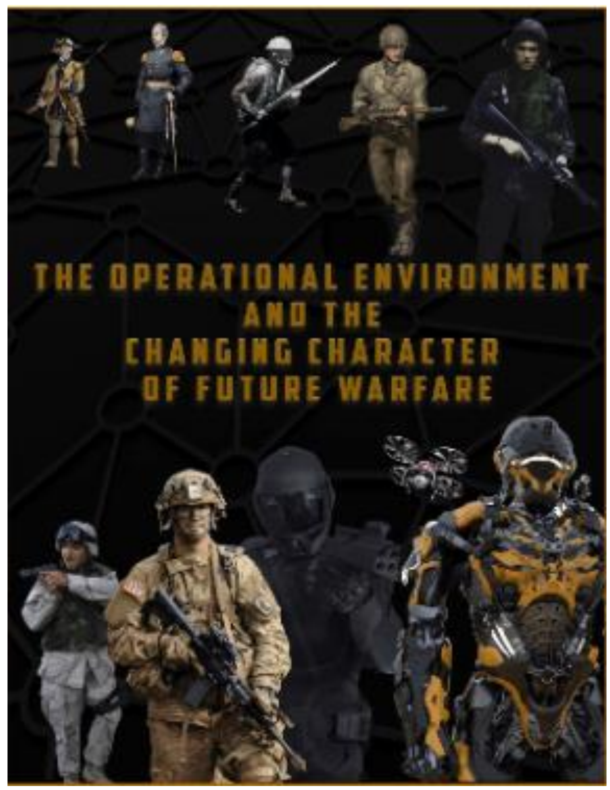
Return to the Table of Contents

Mad Scientist Laboratory Blog Post 46 (19 APR 18)

46. Integrated Sensors: The Critical Element in Future Complex Environment Warfare

(**Editor's Note:** Mad Scientist Laboratory is pleased to present the following guest blog post by **Mr. Richard Nabors**, Associate Director for Strategic Planning and Deputy Director, Operations Division, U.S. Army Research, Development and Engineering Command (RDECOM) Communications-Electronics Research, Development and Engineering Center (CERDEC), addressing how the proliferation of sensors, integrated via the Internet of Battlefield Things [IoBT] will provide Future Soldiers with the requisite situational awareness to fight and win in increasingly complex and advanced battlespaces.)

"*As in preceding decades, that which can be found, if unprotected, can still be hit. By mid-Century, it will prove increasingly difficult to stay hidden. Most competitors can access space-based surveillance, networked multi-static radars, drones and swarms of drones in a wide variety, and a vast of array of passive and active sensors that are far cheaper to produce than to create technology to defeat them. Quantum computing and quantum sensing will open new levels of situational awareness. Passive sensing, especially when combined with artificial intelligence and big-data techniques may routinely outperform active sensors. These capabilities will be augmented by increasingly sophisticated civilian capabilities, where commercial imagery services, a robust and mature Internet of Things, and near unlimited processing power generate a battlespace that is more transparent than ever before.* — **The Operational Environment and the Changing Character of Future Warfare**



The **complex operational environment** of the next conflict cannot be predicted accurately. It has become a **battlespace** — jungle, forest, city, desert, arctic and cyber — where the **enemy is already entrenched** and knows the operational environment. **Complex** and **congested environments** level the field between the United States and its adversaries. The availability of **integrated sensor networks** and **technologies** will be a critical factor in **piercing** the **complexity** of these **environments** and determining what level of **military superiority** is enjoyed by any one side.

As **Soldiers** in complex operational situations are presented with **significantly more information** than in the past and in a broader variety; they have the need to **quickly** and **decisively adapt** to the changing situation, but often do not have the time to sort and judge the value of the information received.

Integrated sensor technologies will provide **situational awareness** by:

• Collecting and sorting **real-time data** and sending a **fusion** of **information** to the **point of need** by **enhancing human vision**,

• **Integrating** with **computers** to detect and identify items of interest in real-time,

• Using **augmented reality** to overlay computer vision with human vision, and

• **Fusing data** together from **multiple sensor sources**.

Networks of sensors integrated with **autonomous systems** will work autonomously to support local operations as well as converge and diverge as needed, **accelerating human decision-making** to the **fastest rates possible** and **maximizing** the **U.S. military's advantage**.

Expected **advances** in Army **sensing capabilities** will directly address **operational vulnerabilities** in **future environments**, including **intelligence, surveillance** and **reconnaissance (ISR)** by a concealed enemy, and **poor visibility** and **short lines of sight** in **urban environments**. These sensors will provide local ISR by **collecting, sorting,** and **fusing real-time data** and sending it to the **point of need**, expanding the **small units' ability** to **sense the adversary**, and providing an **understanding** of the operational environment that the **adversary lacks**.

There are several **technical challenges** that are being addressed in order to **maintain** and **secure overmatch capabilities**. These include:

• **Fusion** of **disparate sensors** into a combined capability.

• **Tactical computing** resources.

• Network **connectivity** and **bandwidth**.

• Sensor suitability for **environmental observation**.

• Reduced **power requirements**.

• Tailored, individual mechanisms through "**sensored**" Soldiers.

• Disguised **unmanned systems** to gather and communicate intelligence.

Future research will focus on **automation** that could track and react to a Soldier's changing situation by **tailoring** the **augmentation** the Soldier receives and by coordinating across the unit. In long-term development, **sensors** on **Soldiers** and **vehicles** will provide **real-time status** and **updates**, optimizing **individually tailored performance levels**. Sensors will provide **adaptive camouflage** for the individual Soldier or platform in addition to **reactive self-healing armor**. The Army will be able to **monitor** the **health** of each Soldier in real-time and **deploy portable autonomous medical treatment centers** using sensor-equipped robots to **treat injuries**. Sensors will enhance detection through **air-dispersible microsensors**, as well as **microdrones** with **image-processing** capabilities.

Image credit: Alexander Kott

In complex environments, the gathering and fusion of information will lead to **greater understanding**. Integrated sensors, remote and near, manned and unmanned, can both **save Soldiers' lives** and make them **more lethal**.

Read about how Russia is trying to increase its number of electro-optical satellites in the ***OE Watch*** November 2017 issue (page 17).

Listen to **Modern War Institute***'s* ***podcast*** where Retired Maj. Gen. David Fastabend and Mr. Ian Sullivan address ***Technology and the Future of Warfare***.

Dr. Richard Nabors *is Associate Director for Strategic Planning, US Army CERDEC Night Vision and Electronic Sensors Directorate.*

Return to the Table of Contents

Chapter 3. Innovation

Return to the Table of Contents

This page intentionally left blank

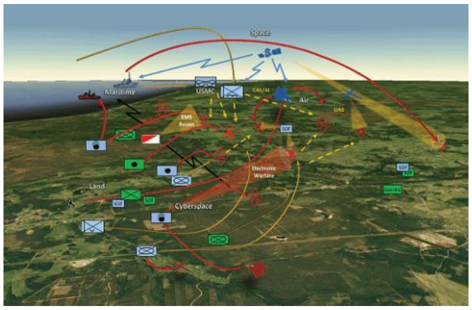
Mad Scientist Laboratory Blog Post 59 (07 June 18)

59. Fundamental Questions Affecting Army Modernization

[**Editor's Note:** The Operational Environment (OE) is the start point for Army Readiness – now and in the Future. The OE answers the question, "What is the Army ready for?" Without the OE in training and Leader development, Soldiers and Leaders are "practicing" in a benign condition, without the requisite rigor to forge those things essential for winning in a complex, multi-domain battlefield. Building the Army's future capabilities, a critical component of future readiness, requires this same start point. The assumptions the Army makes about the Future OE are the *sine qua non* start point for developing battlefield systems — these assumptions must be at the forefront of decision-making for all future investments.]

There are no facts about the future. Leaders interested in building **future ready organizations** must develop assumptions about ***possible*** futures and these assumptions require constant scrutiny. Leaders must also make decisions based on these assumptions to posture organizations to take advantage of opportunities and to mitigate risks. Making these decisions is fundamental to **building future readiness**.

The TRADOC G-2 has made the following foundational assumptions about the future that can serve as launch points for important questions about capability requirements and capabilities under development. These assumptions are further described in ***An Advanced Engagement Battlespace: Tactical, Operational and Strategic Implications for the Future Operational Environment***, published by our colleagues at ***Small Wars Journal***.

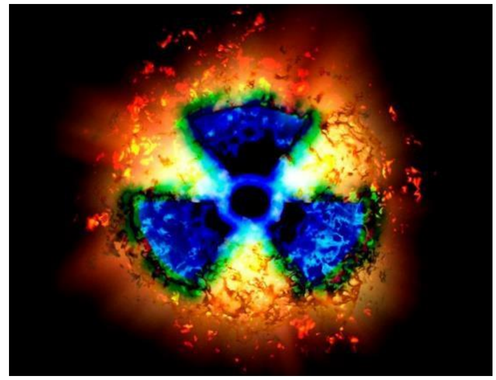


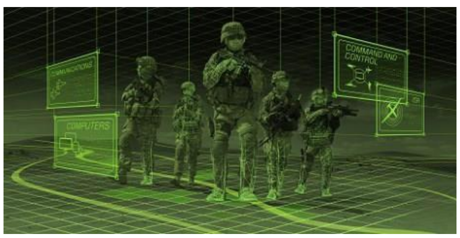
1. Contested in all domains (air, land, sea, space, and cyber). Increased lethality, by virtue of **ubiquitous sensors**, proliferated precision, high kinetic energy weapons and advanced area munitions, further enabled by **autonomy**, **robotics**, and **Artificial Intelligence (AI)** with an increasing potential for overmatch. Adversaries will restrict us to temporary windows of advantage with periods of physical and electronic isolation.

2. Concealment is difficult on the future battlefield. Hiding from advanced sensors — where practicable — will require dramatic reduction of heat, electromagnetic, and optical signatures. Traditional *hider* techniques such as camouflage, deception, and concealment will have to extend to "cross- domain obscuration" in the cyber domain and the electromagnetic spectrum. Canny competitors will monitor their own emissions in real-time to understand and mitigate their vulnerabilities in the "battle of signatures." Alternately, "hiding in the open" within complex terrain clutter and near-constant relocation might be feasible, provided such relocation could outpace future recon / strike targeting cycles. Adversaries will operate among populations in **complex terrain**, including **dense** **urban areas**.

3. Trans-regional, gray zone, and hybrid strategies with both regular and irregular forces, criminal elements, and terrorists attacking our weaknesses and mitigating our advantages. The ensuing spectrum of competition will range from peaceful, legal activities through violent, mass upheavals and civil wars to traditional state-on-state, unlimited warfare.

4. Adversaries include states, non-state actors, and [super-empowered individuals](#), with non-state actors and super empowered individuals now having access to Weapons of Mass Effect (WME), cyber, space, and Nuclear/Biological/ Chemical (NBC) capabilities. Their operational reach will range from tactical to global, and the application of their impact from one domain into another will be routine. These advanced engagements will also be interactive across the multiple *dimensions* of conflict, not only across every domain in the physical dimension, but also the cognitive dimension of information operations, and even the moral dimension of belief and values.





5. Increased speed of human interaction, events and action with **[democratized and rapidly proliferating capabilities](#)** means constant co-evolution between competitors. Recon / Strike effectiveness is a function of its sensors, shooters, their connections, and the targeting process driving decisions. Therefore, in a contest between peer competitors with comparable capabilities, advantage will fall to the one that is better integrated and makes better and faster decisions.

These assumptions become useful when they translate to **potential decision criteria** for Leaders to rely on when evaluating systems being developed for the future battlefield. Each of the following questions are **fundamental** to ensuring the Army is **prepared to operate in the future**.

1. How will this system operate when disconnected from a network? Units will be disconnected from their networks on future battlefields. Capabilities that require constant timing and precision geo-locational data will be prioritized for disruption by adversaries with capable EW systems.

2. What signature does this system present to an adversary? It is difficult to hide on the future battlefield and temporary windows of advantage will require formations to reduce their battlefield signatures. Capabilities that require constant multi-directional broadcast and units with large mission command centers will quickly be targeted and neutralized.

3. How does this system operate in dense urban areas? The physical terrain in dense urban areas and megacities creates concrete canyons isolating units electronically and physically. Automated capabilities operating in dense population areas might also increase the rate of false signatures, confusing, rather than improving, Commander decision-making. New capabilities must be able to operate disconnected in this terrain. Weapons systems must be able to slew and elevate rapidly to engage vertical targets. Automated systems and sensors will require significant training sets to reduce the rate of false signatures.

4. How does this system take advantage of open and modular architectures? The rapid rate of technological innovations will offer great opportunities to militaries capable of rapidly integrating prototypes into formations. Capabilities developed with open and modular architectures can be upgraded with autonomous and AI enablers as they mature. Early investment in closed- system capabilities will freeze Armies in a period of rapid co-evolution and lead to overmatch.

5. How does this capability help win in competition short of conflict with a near peer competitor? Near peer competitors will seek to achieve limited objectives **short of direct conflict** with the U.S. Army. Capabilities will need to be effective at operating in the gray zone as well as serving as deterrence. They will need to be capable of strategic employment from CONUS-based installations.

If you enjoyed this post, check out the following items of interest:

- Join **SciTech Futures**‘ community of experts, analysts, and creatives on 11-18 June 2018 as they discuss the logistical challenges of urban campaigns, both today and on into 2035. What disruptive technologies and doctrines will blue (and red) forces have available in 2035? Are unconventional forces the future of urban combat? Their next ideation exercise goes live 11 June 2018 — click **here** to learn more!

- Watch the U.S. Army Natick Soldier RD&E Center‘s The Soldier of the Future Concept video (the source of the featured image at the top of today’s post).

- View the TRADOC G-2 Operational Environment Enterprise’s The Changing Character of Future Warfare video.

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 20 (16 Jan 18)

20. Building Future Ready Organizations

During the 2017 Mad Scientist Conference on **Robotics, Artificial Intelligence and Autonomy** at Georgia Tech Research Institute, notable futurist Dr. James Canton challenged the audience with an interesting question, **"Are your organizations future ready?"** It seems this simple question drives all of our work to improve strategic foresight and anticipate challenges and opportunities. But how does this question translate into organizational culture and action?

For the United States Army, the case for being future ready is connected to our modernization processes and the speed at which we capitalize on windows of opportunity. For a business or corporation, it might be an emerging technology that will change a current business model.

This comes down to whether we want to be an organization like Netflix — embracing the digital revolution to create a new business model and transforming the way consumers obtain video content (away from legacy video box stores, initially to DVDs ordered on-line and received via the U.S. Postal Service, then to streaming original content on-demand); or like Kodak — developing a digital camera in 1975, but dropping it out of fear that it threatened their then lucrative analog film business, thereby missing the digital media wave that would forever change their business model. Netflix was future ready, while Kodak writhed in bankruptcy and suffered a slow, painful decline.

The first step in answering Dr. Canton's question is asking a series of future-oriented questions. These questions frame a start point for building a future ready organization in hypercompetitive environments.

• How does our organization transform to face challenges or opportunities in a rapidly evolving operational environment?

• How does our organization build, retain, and regain decisive advantage in relation to our competitors?

• How does our organization develop the ability to quickly adapt to emerging trends and traditional and non-traditional competitors' actions?

Answering these questions requires an open approach to developing understanding about future possibilities. One commonly held assumption about the future is that diverse teams and a broad range of expertise is needed to gain an understanding of the future and to see the possibilities for achieving advantage. The Mad Scientist team has identified five key attributes to these types of future oriented teams:

• ***Building*** globally connected, distributed subject matter expert networks. Knowledge is the currency of future oriented organizations and much of it exists outside of any one organization.

• ***Developing*** a network of idea creation that moves the most promising to low cost experimentation. The wisdom of the crowd is essential for broad, creative, and less constrained idea development and for quickly cutting through bureaucratic and cultural roadblocks.

• ***Creating*** networks of teams that feel supported while simultaneously supporting other parts of the organization. Successful teams of teams often are not bound by hierarchical relationships.

• ***Brokering*** ideas and then connecting them to innovation ongoing across an organization. Many future oriented organizations have a hub that connects innovation sparks to further invention and ideas, which can create exponential improvement.

• ***Partnering*** across the organization to move innovative ideas to those who can actualize concepts and deliver results. Large organizations can take some lessons from venture capitalists sponsoring and connecting partners who can quickly transform ideas into low-cost experimentation and results.

Making your organization future ready requires a **deliberate approach** in thinking about the future, **a culture** that improves idea creation, and a structure that **moves ideas to action quickly**. Asking future-oriented questions and building, developing, creating, brokering, and partnering takes these answers and creates **purposeful action**. Instilling future readiness in your organization does not equivocally divert your focus from current and near-term operations and planning; thoughtful intention and attention on the future **insulates organizations from rapid obsolescence**.

To hear more about being a future-oriented organization, watch Dr. James Canton's **presentation** at the Georgia Tech Mad Scientist Conference.

Also, watch Boston Consulting Group's Allison Sander's **TED talk** on mega trends and inevitable futures.

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 50 (07 May 18)

50. Four Elements for Future Innovation

(**Editor's Note:** Mad Scientist Laboratory is pleased to present a new post by returning guest blogger **Dr. Richard Nabors** addressing the four key practices of innovation. Dr. Nabors' previous guest posts discussed how **integrated sensor systems** will provide Future Soldiers with the requisite situational awareness to fight and win in increasingly complex and advanced battlespaces, and how **Augmented and Mixed Reality** are the critical elements required for these integrated sensor systems to become truly operational and support Soldiers' needs in complex environments.)

For the U.S. military to maintain its **overmatch** capabilities, **innovation** is an **absolute necessity**. As noted in **The Operational Environment and the Changing Character of Future Warfare**, our **adversaries** will continue to **aggressively pursue rapid innovation** in key technologies in order to **challenge U.S. forces across multiple domains**. Because of its vital necessity, **U.S. innovation** cannot be left solely to the development of **serendipitous discoveries**.

The Army has successfully generated **innovative** programs and transitioned them from the **research community** into **military use**. In the process, it has identified **four key practices** that can be used in the future development of innovative programs. These practices – **identifying the need, the vision, the expertise,** and **the resources** – are essential in **preparing for warfare** in the **Future Operational Environment**. The recently completed **Third Generation Forward Looking Infrared (3rd Gen FLIR) program** provides us with a **contemporary use case** regarding how each of these practices are key to the **success** of **future innovations**.

1. Identifying the NEED:
To **increase speed, precision,** and **accuracy** of a **platform lethality**, while at the same time **increasing mission effectiveness** and **warfighter safety** and **survivability**.

As the U.S. Army Training and Doctrine Command (TRADOC) noted in its **Advanced Engagement Battlespace** assessment, **future Advanced Engagements** will be…
… **compressed in time**, as the speed of weapon delivery and their associated effects accelerate enormously;
… **extended in space**, in many cases to a global extent, via precision long-range strike and interconnectedness, particularly in the information environment;
… **far more lethal**, by virtue of ubiquitous sensors, proliferated precision, high kinetic energy weapons and advanced area munitions;
… **routinely interconnected** – and contested — **across the multiple domains** of air, land, sea, space and cyber; and
… **interactive across the multiple dimensions of conflict**, not only across every domain in the physical dimension, but also the cognitive dimension of information operations, and even the moral dimension of belief and values.

Identifying the NEED within the context of these **future Advanced Engagement characteristics** is critical to the success of **future innovations**.

The first-generation FLIR systems gave a limited ability to detect objects on the battlefield at night. They were large, slow, and provided low-resolution, short-range images. The need was for **greater speed, precision,** and **range** in the targeting process to unlock the full potential of infrared imaging. **Third generation FLIR** uses multiband infrared imaging sensors combined with multiple fields of view which are integrated with computer software to automatically enhance images in real-time. **Sensors** can be used across **multiple platforms** and **missions**, allowing **optimization** of equipment for battlefield conditions, greatly **enhancing mission effectiveness** and **survivability**, and providing significant cost savings.

2. Identifying the VISION: To **look beyond** the need and what is possible **to what could be possible**.

As we look forward into the **Future Operational Environment**, we must address those **revolutionary technologies** that, when developed and fielded, will provide a decisive edge over adversaries not similarly equipped. These **potential Game Changers** include:

• **Laser and Radio Frequency Weapons** – Scalable lethal and non-Lethal directed energy weapons can counter Aircraft, UAS, Missiles, Projectiles, Sensors, and Swarms.
• **Swarms** – Leverage autonomy, robotics, and artificial intelligence to generate “global behavior with local rules” for multiple entities – either homogeneous or heterogeneous teams.
• **Rail Guns and Enhanced Directed Kinetic Energy Weapons (EDKEW)** – Non explosive electromagnetic projectile launchers provide high velocity/high energy weapons.
• **Energetics** – Provides increased accuracy and muzzle energy.
• **Synthetic Biology** – Engineering and modification of biological entities has potential weaponization.
• **Internet of Things** – Linked internet “things” create opportunity and vulnerability. Great potential benefits already found in developing U.S. systems also create a vulnerability.
• **Power** – Future effectiveness depends on renewable sources and reduced consumption. Small nuclear reactors are potentially a cost-effective source of stable power.

Understanding these **Future Operational Environment Game Changers** is central to **identifying the VISION** and looking beyond the need to **what could be possible**.

The 3rd Gen FLIR program struggled early in its development to **identify requirements** necessary to sustain a successful program. Without the **user community**’s understanding of a **vision** of **what could be possible**, requirements were based around the **perceived limitations** of what technology could provide. To overcome this, the research community developed a **comprehensive strategy** for **educational outreach** to the Army’s **requirement developers, military officers,** and **industry** on the full potential of what 3rd Gen FLIR could achieve. This campaign **highlighted** not only the recognized need, but also a **vision** for what was possible, and served as the **catalyst** to bring the entire community together.

3. Identifying the EXPERTISE:
To gather expertise from **all possible sources** into a **comprehensive solution**.

Human creativity is the **most transformative force** in the world; people **compound** the **rate of innovation** and **technology development**. This expertise is fueling the **convergence** of technologies that is already leading to **revolutionary achievements** with respect to **sensing, data acquisition** and **retrieval**, and **computer processing hardware**.

Identifying the EXPERTISE leads to the **exponential convergence** and **innovation** that will **afford strategic advantage** to those who recognize and leverage them.

The **expertise** required to achieve 3rd Gen FLIR success was from the **integration** of more than 16 significant research and development projects from **multiple organizations**: Small Business Innovation Research programs; applied research funding, partnering in-house expertise with external communities; Manufacturing Technology (ManTech) initiatives, working with manufacturers to develop the technology and long-term manufacturing capabilities; and advanced technology development funding with traditional large defense contractors. The **talented workforce** of the Army research community **strategically aligned** these individual activities and worked with them to provide a **comprehensive, interconnected final solution**.

4. Identifying the RESOURCES:
To consistently **invest** in innovative technology by **partnering** with others to **create multiple funding sources**.

The **2017 National Security Strategy** introduced the **National Security Innovation Base** as a critical component of its vision of American security. In order to meet the challenges of the Future Operational Environment, the Department of Defense and other agencies must establish **strategic partnerships** with U.S. companies to help align **private sector Research and Development (R&D) resources** to priority national security applications in order to **nurture innovation**.

The development of 3rd Gen FLIR took many years of **appropriate, consistent investments** into innovations and technology breakthroughs. Obtaining the **support of industry** and leveraging their internal **R&D investments** required the Army to **build trust** in the overall program. By **creating partnerships** with others, such as the U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) and ManTech, 3rd Gen FLIR was able to **integrate multiple funding sources** to ensure a **secure resource foundation**.

CONCLUSION
The successful 3rd Gen FLIR program is a **prototype** of the **implementation** of an **innovative program**, which transitions good ideas into actual capabilities. It exemplifies how **identifying the need, the vision, the expertise** and **the resources** can create an

environment where **innovation thrives**, equipping warriors with the **best technology** in the world. As the Army looks to increase its **exploration** of **innovative technology development** for the future, these examples of **past successes** can serve as **models** to build on moving forward.

See our **Prototype Warfare** post to learn more about **other contemporary innovation successes** that are helping the U.S. maintain its competitive advantage and win in an **increasingly contested Operational Environment**.

Dr. Richard Nabors *is Associate Director for Strategic Planning and Deputy Director, Operations Division, U.S. Army Research, Development and Engineering Command (RDECOM) Communications-Electronics Research, Development and Engineering Center (CERDEC), Night Vision and Electronic Sensors Directorate.*

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 12 (18 Dec 17)

12. Prototype Warfare

But in the future, mass production of the implements of war will not work. Technological advancements happen too fast in the Information Age.… Instead, the future of materiel acquisition will be the rapid development and fielding of prototypes.” – Robert R. Leonhard, **The Principles of War for the Information Age**, Presidio Press, Novato, CA, 1998, pp. 122-123.

The character of warfare is largely reflective of the character and changes within society and technology. The pace of changes and advancements in technology is accelerating quickly due to the convergence of a multitude of technologies. This ever-quickening pace of technological evolution means the Army must adapt and change at a speed that cannot currently be applied across the entire force. This conundrum brings about the possible efficacy of *prototype warfare*.

Prototype warfare is the concept of quickly developing and fielding technologies to rapidly adapt to a changing Operational Environment (OE) and emerging Tactics, Techniques, and Procedures (TTPs), as well as overcoming shortcomings or challenges in manpower, capability, and reach. One hurdle to prototype warfare is a byzantine acquisition process that limits the rapid acquisition and fielding of new technologies to the force until the associated documentation has completed its circuitous trek through a multi-tiered approval process and its funding has been programmed.

But every brigade in the Army may not need that particular technology or kit. ***Modularity*** is essential in prototype warfare. For instance, when one considers the emerging discussion and heavy investment modular pieces of future exoskeletons that may be ready now and can be fielded to Army units that need it. If the heavy-lift support or burden-lessening legs portion of an exoskeleton are practically functional at this time, a unit like 10th Mountain Division could use such a technology to lessen the likelihood of muscular-skeletal injuries from heavy loads being carried during training and operations.

Furthermore, as described in **An Advanced Engagement Battlespace: Tactical, Operational and Strategic Implications for the Future Operational Environment**, the future OE will be characterized by *tactical pulsing* (i.e., “sudden extreme pulses of violent offensive action”). Unlike the great conflicts of the previous century, those in the 21st Century will not afford belligerents the relative luxury of ramping up their production capacities from a consumer to a war economy. Our Arsenal of Democracy, churning out long-range bombers, tanks, and ships by the thousands, has no contemporary relevancy. As Mr. Leonhard eloquently points out in his book, **The Principles of War for the Information Age**:

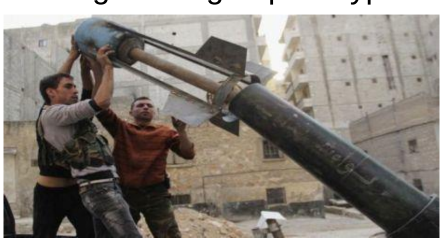
"We must declare with finality that we have overcome the limitations and inefficiencies of mass warfare, and that we are determined to leave it behind. Mass is dead."

In Mr. Robert Kozloski's "**The Path to Prototype Warfare**," posted in **War on the Rocks**, July 17, 2017, he states:

"Deploying many varieties of prototypes… create[s] a significant dilemma for a defender, thus presenting an advantage for an attacker…. These prototypes may be produced at a lower cost and may only need to be operational for a short time period."

Prototype warfare will provide the requisite agility in delivering the required capabilities to execute tactical pulsing in the future OE, enabling us to inflict *"paroxysms of intense, hyperactive violence"* upon our adversaries.

The convergence of a number of emerging technologies – synthetic prototyping, additive manufacturing, advanced modeling and simulations, software-defined everything, advanced materials – are advancing the feasibility of prototype warfare. Simultaneously, however, it is also democratizing this approach, enabling and improving the engineering of prototype weapons by non-state actors and super-empowered individuals. In his article posted in ***Wired*** this week, Mr. Brian Castner reports that ISIS is already *"design[ing] their own munitions and mass-produc[ing] them using advanced manufacturing techniques. Iraq's oil fields provided the industrial base—tool-and-die sets, high-end saws, injection-molding machines—and skilled workers who knew how to quickly fashion intricate parts to spec. Raw materials came from cannibalizing steel pipe and melting down scrap. ISIS engineers forged new fuzes, new rockets and launchers, and new bomblets to be dropped by drones, all assembled using instruction plans drawn up by ISIS officials."*



The following are examples of recent U.S. prototype warfare successes:

Combined Joint Task Force Paladin, activated to swiftly research and develop countermeasures to improvised explosive devices (IEDs), is a great example of prototype warfare. Extrapolating this generality of rapid acquisition would be beneficial to U.S. forces and could provide overmatch in niche areas.

The United States Special Operations Command's **SOFWERX** was created in 2015 in a joint effort with the Doolittle Institute to be an open-door technological incubator where academics, techies, tinkerers, and researchers work together to get emerging tech out and into the hands of special operators. Due to its success and unique innovation, SOFWERX is the shining beacon for rapid acquisition within the DoD.

DoD is venturing into prototype warfare with **Project Maven** (also known as the Algorithmic Warfare Cross Functional Team), an effort launched by former Deputy Secretary of Defense Bob Work, to accelerate the department's integration of big data, artificial intelligence (AI) and machine learning (ML). The primary focus of the program is to overcome the tyranny of man-hours and effort required to analyze an enormous volume of full motion video with AI/ML. The existing process is human-driven, tedious, and susceptible to errors in perception and monotony. LTG John "Jack" Shanahan (USAF) spoke about prototype warfare in a keynote speech at NVIDIA's GPU Technology Conference in November, highlighting the importance of having big goals, winning small victories early, and keeping focus. Project Maven is currently expecting to deliver the first algorithms to warfighting systems by the end of the year. The team is already looking to the next set of "sprints" to tackle more intelligence analytics challenges and opportunities.

"[Project Maven] is about moving from the hardware industrial age to a software data-driven information environment and doing it fast and at scale across the Department."
— LTG Shanahan.

Prototype warfare is often dismissed as something relegated to the smaller, more narrowly focused special operations forces and not applicable to conventional forces. However, if the Army is to maintain its competitive advantage and win in an increasingly contested operational environment with continually evolving technologies, it must explore the potential of prototype warfare.

In doing so, the following questions must be considered:

1) How can the Army embrace prototype warfare without disrupting current acquisition processes that are in place to ensure security, reliability, and compliance in fielding required capabilities?

2) Should prototype warfare be spread across the Services or should it be centralized within a single organization?

3) What are the potential drawbacks and limitations in prototype warfare? What are the unforeseen second and third order effects of such a process?

For further reading on this subject, see the following recent articles:

SOCOM Procurement Mantra: Lighter, Quicker, Cheaper

Special Ops Command Woos Nontraditional Technology Developers

Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges

Say Hello to Alrobot, Iraq's Homebuilt War Robot

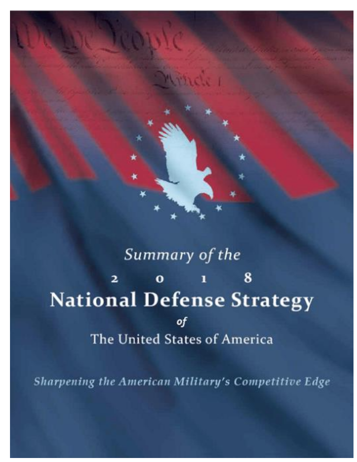
Return to the Table of Contents

Mad Scientist Laboratory Blog Post 60 (11 June 18)

60. Mission Engineering and Prototype Warfare: Operationalizing Technology Faster to Stay Ahead of the Threat

[**Editor's Note:** Mad Scientist is pleased to present the following post by a team of guest bloggers from **The Strategic Cohort** at the **U.S. Army Tank Automotive Research, Development, and Engineering Center (TARDEC)**. Their post lays out a clear and cogent approach to Army modernization, in keeping with the Chief of Staff of the Army GEN Mark A. Milley's and Secretary of the Army Mark T. Esper's guidance "*to focus the Army's efforts on delivering the weapons, combat vehicles, sustainment systems, and equipment that Soldiers need when they need it"* and making *"our Soldiers more effective and our units less logistically dependent*." — **The Army Vision**, 06 June 2018]

"Success no longer goes to the country that develops a new fighting technology first, but rather to the one that better integrates it and adapts its way of fighting…." – **The National Defense Strategy** (2018).



Executive Summary

While Futures Command and legislative changes streamline acquisition bureaucracy, the Army will still struggle to keep pace with the global commercial technology marketplace as well as innovate ahead of **adversaries** who are also innovating.

Reverse engineering and technology theft make it possible for adversaries to inexpensively copy DoD-specific technology "widgets," potentially resulting in a "negative return" on investment of DoD research dollars. Our adversaries' pace of innovation further compounds our challenge. Thus the Army must not only equip the force to confront what is expected, but equip the force to confront an adaptable enemy in a wide variety of environments. This paper proposes a framework that will enable identification of strategically relevant problems and provide solutions to those problems at the speed of relevance and invert the cost asymmetry.

To increase the rate of innovation, the future Army must learn to continually assimilate, produce, and operationalize technologies much faster than our adversaries to gain time-domain overmatch. The overarching goal is to create an environment that our adversaries cannot duplicate: integration of advanced technologies with skilled Soldiers and well-trained teams. The confluence of two high level concepts — the Office of the Secretary of Defense's **Mission Engineering** and Robert Leonard's **Prototype Warfare** (see his **Principles of Warfare for the Information Age** book) — pave the way to increasing the rate of innovation by operationalizing technology faster to stay ahead of the threat, while simultaneously reducing the cost of technology overmatch.

Mission Engineering

OSD's **Mission Engineering** concept, proposed by Dr. Robert Gold, calls for acquisitions to treat the end-to-end mission as the system to optimize, in which individual systems are components. Further, the concept utilizes an assessment framework to measure progress towards mission accomplishment through test and evaluation in the mission context. In fact, all actions throughout the capability development cycle must tie back to the mission context through the assessment framework. It goes beyond just sharing data to consider functions and the strategy for trades, tools, cross-cutting functions, and other aspects of developing a system or system of systems.

Consider the example mission objective of an airfield seizure. Traditional thinking and methods would identify an immediate needed capability for two identical air droppable vehicles, therefore starting with a highly constrained platform engineering solution. Mission Engineering would instead start by asking: what is the best way to seize an airfield? What mix of capabilities are required to do so? What mix of vehicles (e.g., Soldiers, exoskeletons, robots, etc.) might you need within space and weight constraints of the delivery aircraft? What should the individual performance requirements be for each piece of equipment?

Mission Engineering breaks down cultural and technical "**domain stovepipes**" by optimizing for the mission instead of a ground, aviation, or cyber specific solution. There is huge innovation space between the conventional domain seams.

For example, ground vehicle concepts would be able to explore looking more like motherships deploying exoskeletons, drone swarms, or other ideas that have not been identified or presented because they have no clear home in a particular domain. It warrants stating twice that **there are a series of mission optimized solutions that have not been identified or presented because they have no clear home in the current construct.** Focusing the enterprise on the mission context of the problem set will enable solutions development that is relevant and timely while also connecting a network of innovators who each only have a piece of the whole picture.

Prototype Warfare

Prototype Warfare represents a paradigm shift from fielding large fleets of common-one-size-fits-all systems to rapidly fielding small quantities of tailored systems. Tailored systems focus on specific functions, specific geographic areas, or even specific fights and are inexpensively produced and possibly disposable.

For example, vehicle needs are different for urban, desert, and mountain terrains. A single system is unlikely to excel across those three terrains without employing exotic and expensive materials and technology (becoming expensive and exquisite). They could comprise the entire force or just do specific missions, such as **Hobart's Funnies** during the D-Day landings.

A further advantage of tailored systems is that they will force the enemy to deal with a variety of unknown U.S. assets, perhaps seen for the first time. A tank platoon might have a heterogeneous mix of assets with different weapons and armor. Since protection and lethality will be unknown to the enemy, it will be asymmetrically challenging for them to develop in a timely fashion tactics, techniques, and procedures or materiel to effectively counter such new capabilities.

Potential Enablers

Key technological advances present the opportunity to implement the Mission Engineering and Prototype Warfare concepts. **Early Synthetic Prototyping (ESP), rapid manufacturing,** and the burgeoning field of **artificial intelligence (AI)** provide ways to achieve these concepts. Each on its own would present significant opportunities. ESP, AI, and rapid manufacturing, when applied within the Mission Engineering/Prototype Warfare framework, create the potential for an **innovation revolution**.

Under development by the Army Capabilities Integration Center (ARCIC) and U.S. Army Research, Development, and Engineering Command (RDECOM), **ESP** is a physics-based persistent game network that allows Soldiers and engineers to collaborate on exploration of the materiel, force structure, and tactics trade space. ESP will generate 12 million hours of digital battlefield data per year.

Beyond the ESP engine itself, the Army still needs to invest in cutting edge research in machine learning and big data techniques needed to derive useful data on tactics and technical performance from the data. Understanding human intent and behaviors is difficult work for current computers, but the payoff is **truly disruptive**. Also, as **robotic systems** become more prominent on the battlefield, the country with the **best AI** to control them will have a great advantage. The best AI depends on having the most training, experimental, and digitally generated data. The Army is also acutely aware of the challenges involved in testing and system safety for AI enabled systems; understanding what these systems are intended to do in a mission context fosters debate on the subject within an agreed upon problem space and associated assessment framework.

Finally, to achieve the vision, the Army needs to invest in technology that allows rapid problem identification, engineering, and fielding of tailored systems. For over two decades, the Army has touted modularity to achieve system tailoring and flexibility.

However, any time something is modularized, it adds some sort of interface burden or complexity. A specific-built system will always outperform a modular system. Research efforts are needed to understand the trade-offs of custom production versus modularity. The DoD also needs to strategically grow investment in new **manufacturing technologies** (to include 3D printing) and **open architectures** with industry.

Associated Implications

New challenges are created when there is a hugely varied fleet of tailored systems, especially for logistics, training, and maintenance. One key is to develop a well-tracked digital manufacturing database of replacement parts. For maintenance, new technologies such as augmented reality might be used to show mechanics who have never seen a system how to rapidly diagnose and make repairs.

New Soldier interfaces for platforms should also be developed that are standardized/simplified so it is intuitive for a soldier to operate different systems in the same way it is intuitive to operate an iPhone/iPad/Mac to reduce and possibly eliminate the need for system specific training. For example, imagine a future soldier gets into a vehicle and inserts his or her common access card. A driving display populates with the Soldier's custom widgets, similar to a smartphone display. The displays might also help soldiers understand vehicle performance envelopes. For example, a line might be displayed over the terrain showing how sharp a soldier might turn without a rollover.

Conclusion

The globalization of technology allows **anyone** with money to purchase "bleeding-edge," militarizable commercial technology. This changes the way we think about the ability to generate combat power to compete internationally from the physical domain, to the time domain. Through the proposed mission engineering and prototype warfare framework, the Army can assimilate and operationalize technology quicker to create an ongoing time-domain overmatch and invert the current cost asymmetry which is adversely affecting the public's will to fight. Placing human thought and other resources towards finding new ways to understand mission context and field new solutions will provide capability at the speed of relevance and help reduce operational surprise through a better understanding of what is possible.

If you enjoyed this post, join **SciTech Futures**' community of experts, analysts, and creatives on 11-18 June 2018 as they discuss the logistical challenges of urban campaigns, both today and on into 2035. What disruptive technologies and doctrines will blue (and red) forces have available in 2035? Are unconventional forces the future of urban combat? Their next ideation exercise goes live today — click **here** to learn more!

This article was written by **Dr. Rob Smith***, Senior Research Scientist;* **Mr. Shaheen Shidfar***, Strategic Cohort Lead;* **Mr. James Parker***, Associate Director;* **Mr. Matthew A. Horning***, Mission Engineer; and* **Mr. Thomas Vern***, Associate Director. Collectively, these gentlemen are a subset of* **The Strategic Cohort***, a multi-disciplinary independent group of volunteers located at TARDEC that study the Army's Operating Concept Framework to understand how we must change to survive and thrive in the future operating environment. The Strategic Cohort analyzes these concepts and other reference materials, then engages in disciplined debate to provide recommendations to improve TARDEC's alignment with future concepts, educate our workforce, and create dialogue with the concept developers providing a feedback loop for new ideas*.

Further Reading:

Gold, Robert. "**Mission Engineering**." 19th Annual NDIA Systems Engineering Conference, Oct. 26, 2016, Springfield, VA. Presentation.

Leonard, Robert R. The Principles of War for the Information Age, Presidio Press (2000).

Martin, A., & FitzGerald, B. "**Process Over Platforms**." Center for a New American Security, Dec. 13, 2013.

FitzGerald, B., Sander, A. & Parziale, J. "**Future Foundry A New Strategic Approach to Military-Technical Advantage**." Center for a New American Security, Dec. 14, 2016.

Kozloski, Robert. "**The Path to Prototype Warfare**." War on the Rocks, 17 July 2017.

Hammes, T.X. "**The Future of Warfare: Small, Many, Smart vs. Few & Exquisite?**" War on the Rocks, 7 Aug. 2015.

Smith, Robert E. "**Tactical Utility of Tailored Systems**." Military Review (2016).

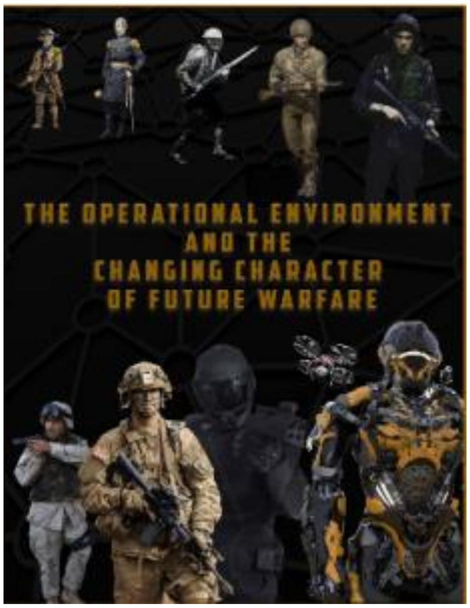
Smith, Robert E. and Vogt, Brian. "**Early Synthetic Prototyping Digital Warfighting For Systems Engineering**." Journal of Cyber Security and Information Systems 5.4 (2017).

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 42 (05 April 18)

42. China's Drive for Innovation Dominance



"While the U.S. military may not necessarily have to fight Russia or China, it is likely that U.S. forces through 2050 will encounter their advanced equipment, concepts, doctrine, and tactics in flashpoints or trouble spots around the globe.." — extracted from **The Operational Environment and the Changing Character of Future Warfare**

The Future Operational Environment's **Era of Contested Equality** (i.e., 2035 through 2050) will be marked by significant breakthroughs in **technology** and **convergences**, resulting in **revolutionary changes** that challenge the very nature of warfare itself. No one actor is likely to have any long-term strategic or technological advantage during this period of **enduring competition**. **Prevailing** in this environment will depend on an ability to **synchronize multi-domain capabilities** against an **artificial intelligence-enhanced** adversary with an overarching capability to **visualize** and **understand** the **battlespace** at even **greater ranges** and **velocities**.

Ms. Elsa Kania, Adjunct Fellow, Technology and National Security Program, Center for a New American Security (CNAS), presented **"*People's Liberation Army (PLA) Human-Machine Integration"*** at last month's **Bio Convergence and Soldier 2050 Conference**. In this presentation, Ms. Kania addressed China's on-going initiatives that seek to change military power paradigms via competition and innovation in a number of key technologies. This post summarizes Ms. Kania's presentation.

Under **President Xi Jinping**'s leadership, China is becoming a **major engine** of **global innovation**, second only to the United States. China's national strategy of **"innovation-driven development"** places innovation at the forefront of **economic** and **military development**. These efforts are beginning to pay off, as **Beijing** is becoming **as innovative as Silicon Valley**. China continues to strengthen its military through a series of ambitious **Science and Technology (S&T) plans** and **investments**, focusing on

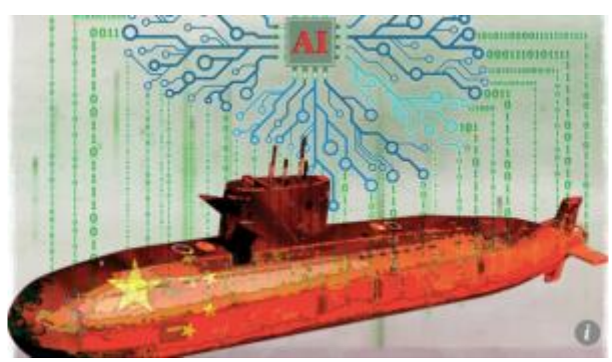
disruptive and **radical innovations** that will enable them to seize the high ground with **decisive technologies** (e.g., AI, hypervelocity, and biotechnology).

President Xi leads China's **Central Military-Civil Fusion Development Commission**, whose priorities include intelligent unmanned systems, biology and cross-disciplinary technologies, and quantum S&T. Though the implementation of a **"whole of nation" strategy**, President Xi is leveraging private sector advances for military applications. This strategy includes the establishment of **Joint Research Institutes** to promote **collaborative R&D**; **new national labs** focused on achieving **dual-use advances**; and collaboration within **national military-civil fusion innovation demonstration zones**. Major projects concentrate on **quantum communications** and **computing, brain science,** and **brain-inspired research**.

By 2030, China will be **world's premier Artificial Intelligence (AI) innovation center**. Building upon their successes with Alpha Go, the PLA is seeking to establish a **"Battlefield Singularity,"** leveraging AI potential in planning, operational command and control, decision support tools, wargaming, and brain-computer interfaces controlling unmanned systems. They will **deepen military-civil fusion AI initiatives** with **Baidu, Alibaba Group, Tencent,** and **iFLYTEK. AI** is seen as a potential **game-changer** by the Chinese, a way to **augment perceived military shortcomings**.

This focused initiative on innovation may result in **China's First Offset**, characterized by integrating quantum satellites with fiber optic communication networks; **human-machine interfaces**; drone swarms able to target carrier task forces; naval rail guns; and quantum computing.

Potential areas for **biotechnology** and **AI convergences** include:



• **"Intelligentized" Command Decision-Making:** The Joint Staff Department of the **Central Military Commission (CMC)** has called for the PLA to leverage the "**tremendous potential**" of AI in planning, operational command, and decision support. Ongoing research is focusing on **command automation** and "**intelligentization**," with experimental demonstrations of an **"external brain"** for commanders and **decision support systems** for fighter pilots and submarines.

• **Brain-Computer Interfaces:** Active research programs in **brain-computer interfaces** are underway (e.g., at PLA Information Engineering University, Tsinghua University), enabling "**brain control**" of **robotic** and "**unmanned**" systems and potentially facilitating **brain networking**.

• **Military Exoskeletons:** Several **prototype exoskeletons** have been tested and demonstrated to date, augmenting soldiers' physical capabilities, with the **latest generations** being **more capable** and **closer to being fielded** by the PLA.

• **CRISPR in China: Gene editing** is currently underway with **animals** and **human embryos** due to **less stringent regulatory requirements** in the PRC. **BGI** (a would-be "bio-Google") is currently soliciting **DNA from Chinese geniuses** in an attempt to understand the **genomic basis for intelligence**.

• **Chinese Superintelligence:** The Chinese aspire to develop "**brain-like**" or **human-level AI**. Their new **National Engineering Laboratory for Brain-Inspired Intelligence Technologies and Applications**, with **Baidu** involvement, is focusing on learning from the human brain to tackle AI, **advancing next-generation AI technologies.**

While technological advantage has been a key pillar of U.S. military power and national competitiveness, **China is rapidly catching up**. Future **primacy in AI and biotech**, likely **integral in future warfare**, could **remain contested between** the **U.S.** and **China**. The PLA will continue explore and invest in these **key emerging technologies** in their on-going drive for **innovation dominance**.

For more information regarding the PLA's on-going innovation efforts:

Watch Ms. Kania's **video presentation** (and read the associated **slides** from the Bio Convergence and Soldier 2050 Conference.

Listen to Ms. Kania's **China's Quest for Enhanced Military Technology** podcast, hosted by our colleagues at ***Modern War Institute***.

Read Ms. Kania's ***"Battlefield Singularity Artificial Intelligence, Military Revolution, and China's Future Military Power,"*** which can be downloaded **here**.

Check out Ms. Kania's Battlefield Singularity **website**.

Return to the Table of Contents

Chapter 4. Edge Cases

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 41 (02 Apr 18)

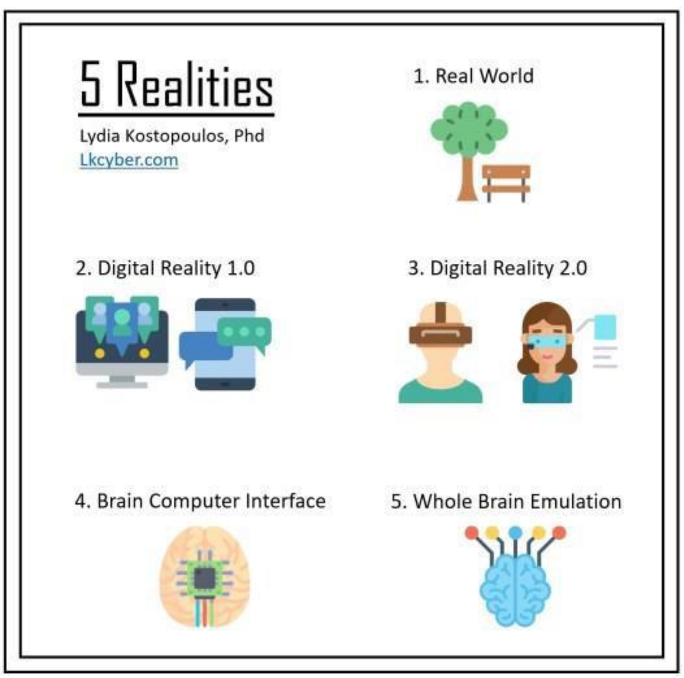
41. The Technological Information Landscape: Realities on the Horizon

(**Editor's Note:** Mad Scientist Laboratory is pleased to present the following guest blog post by **Dr. Lydia Kostopoulos**, addressing the future of technological information and the tantalizing possible realities they may provide us by 2050.)

The **history of technology** and its contemporary developments is not a story about technology, **it is a story about people, politics and culture.** Politics encouraged **military technologies** to be developed which have had **tremendous value** for **civilian use**. Technologies that were too ahead of their cultural times were left behind. As the saying goes 'need is the mother of all inventions', and many **technological advances** have been thanks to the **perseverance** of people who were **determined to solve a problem** that affected **their life**, or that of **their loved ones** and **community.**

Ultimately, technology starts with people, ideas come from people, and the perception of reality is a human endeavor as well.

The **'reality' related technologies** that are part of the current and emerging **information landscape** have the potential to **alter** the **perception of reality**, **form new digital communities** and **allegiances**, **mobilize people**, and **create reality dissonance**. These realities also contribute to the evolving ways that **information** is **consumed, managed,** and **distributed**. There are **five components:**



1. Real World: Pre-internet real, touch-feel-and-smell world.

2. Digital Reality 1.0: There are many already existing **digital realities** that people can immerse themselves into, which include **gaming**, as well as **social media** and worlds such as **Second Life**. Things that happen on these **digital platforms** can affect the **real world** and **visa-versa.**

3. Digital Reality 2.0: The **Mixed Reality (MR)** world of **Virtual Reality (VR)** and **Augmented Reality (AR)**. These technologies are still in their early stages; however, they show **tremendous potential** for **receiving**, and **perceiving information**, as well as **experiencing narratives through synthetic or captured moments**.

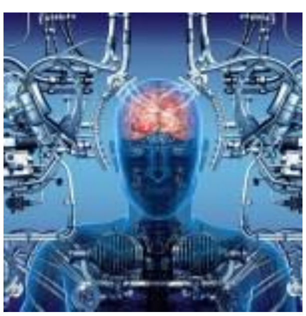
Virtual Reality allows the user to step in a "virtual" reality, which can be **entirely synthetic** and a **created digital environment,** or it could be a **suspended moment** of an actual real-world environment. The **synthetic environment** could be modeled after the real world, a fantasy, or a bit of both. Most virtual realities do not fully cross over the **uncanny valley**, but it is only a matter of time. Suspended moments of actual real-world environments involve 360 degree cameras which capture a video moment in time; these already exist and the degree in which it feels like the VR user is **teleported** to that **geographical and temporal moment in time** will, for the most part, depend on the quality of the video and the sound. This VR experience can also be **modified, edited and amended** just like regular videos are edited today. This, coupled with technologies that authentically replicate voice (ex: Adobe VoCo) and

technologies that can change faces in videos, **create open-ended possibilities for 'fake' authentic videos and soundbites** that can be embedded.

Augmented Reality allows the user to interact with a digital layer superimposed on their physical real world. The technology is still in the early stages, but when it reaches

its full potential, **it is expected to disrupt and transform the way we communicate, work, and interact with our world.** Some say the combination of **voice command, artificial intelligence, and AR will make screens a thing of the past.** Google is experimenting with their new app, **Just a Line**, which allows the users to play with their augmented environment and **create digital graffiti** in their physical space. While this is an **experiment**, the **potential** for **geographic AR experiences, messages** (overt or covert), and **storytelling** is **immense.**

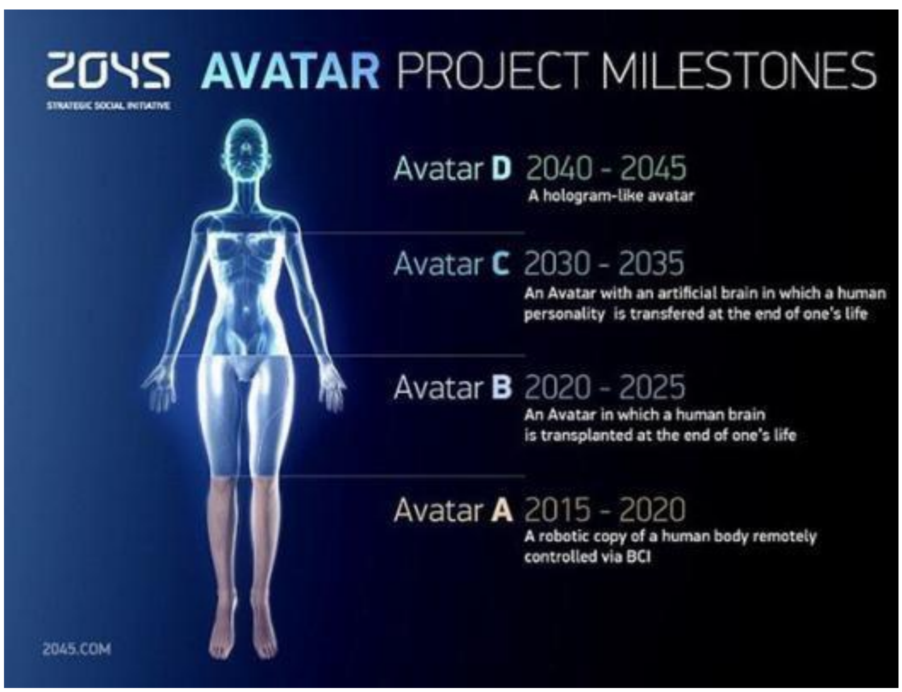
4. Brain Computer Interface (BCI): Also called **Brain Machine Interface (BMI).** BCI has the potential to **create another reality** when the **brain** is **seamlessly connected** to the **internet**. This may also **include connection** to **artificial intelligence** and **other brains**. This technology is currently being developed, and the space for **'minimally invasive' BCI** has **exploded.** Should it work as intended, the user would, in theory, **be directly communicating** to the **internet through thought**, the **lines would blur** between the **user's memory and knowledge** and



the **augmented intelligence** its brain accessed in real-time through BCI. In this sense it would also be able to communicate **with others through thought using BCI as the medium.** The **sharing** of information, ideas, memories and emotions through this medium would **create a new way of receiving, creating and transmitting information,** as well as a **new reality experience.** However, for those with a **sinister mind**, this technology could also have the potential to be used as a method for implanting ideas into others' minds and subconscious. For an in-depth explanation on one company's efforts to make BCI a reality, see Tim Urban's post "**Neuralink and the Brain's Magical Future**".

5. Whole Brain Emulation (WBE): Brings a very new dimension to the information landscape. It is very much still in the early stages, however, if successful, this would create a **virtual immortal sentient existence** which would live and interact with the other realities. It is still unclear if the **uploaded mind** would be **sentient**, how it would **interact** with its **new world (the cloud),** and what implications it would have on those who know

or knew the person. As the technology is still new, many avenues for brain uploading are being explored which include it being done while a person is alive and when a person dies. Ultimately a **'copy'** of the mind would be made and the computer would run a **simulation model of the uploaded brain,** it is also expected to have a **conscious mind of its own**. This **uploaded, fully functional brain** could live in a **virtual reality** or in a computer which takes physical form in a **robot** or **biological body**. Theoretically, this technology would allow uploaded minds to **interact with all realities** and be able to **create and share information**.



Apart from another means for communicating with others, and transmitting information, it can also be used as a medium to **further ideologies**. For example, if **Osama bin Laden's brain** had been uploaded to the cloud, his living followers for generations to come could **interact with him** and **acquire feedback and guidance**. Another example is **Adolf Hitler**; if his brain were to have been uploaded, his modern-day followers would be able to **interact** with him through **cognitive augmentation** and **AI**. This of course could be used to 'keep' loved ones in our lives, however the technology has broader implications when it is used to **perpetuate harmful ideologies, shape opinions,** and **mobilize populations** into violent action. As mind-boggling as all this may sound, the WBE "hypothetical futuristic process of scanning the mental state of a particular brain substrate and copying it to a computer" is being scientifically pursued. In 2008, the **Future of Humanity Institute** at **Oxford University** published a technical report about the **roadmap to Whole Brain Emulation**.

Despite the many questions that remain unanswered and a lack of a human brain upload proof of concept, a new startup, **Nectome**, which is **"Committed to the goal of archiving your mind,"** offers a **brain preservation service** and when the technology is available, they will **upload the brains**. In return, the clients pay a service fee of $10,000 and agree for the embalming chemicals to be introduced into their arteries (under general anesthesia) **right before** they pass away, so that the **brain can be freshly extracted**.

These technologies and realities create new areas for **communication, expression** and **self-exploration**. They also provide spaces where **identities transform**, and where the **perception of reality within** and **among these realities** will hover somewhere above these **many identities** as people weave in and through them in their daily life.

For more information regarding **disruptive technologies**, see Dr. Kostopoulos' **blogsite**.

Please also see Dr. Kostopoulos' recent submission to our Soldier 2050 Call for Ideas, entitled ***Letter from the Frontline: Year 2050***, published by our colleagues at ***Small Wars Journal***.

Dr. Lydia Kostopoulos *is an advisor to the AI Initiative at The Future Society at the Harvard Kennedy School, participates in NATO's Science for Peace and Security Program, is a member of the FBI's InfraGard Alliance, and during the Obama administration received the U.S. Presidential Volunteer Service Award for her pro bono work in cybersecurity. Her work lies in the intersection of strategy, technology, education, and national security. Her professional experience spans three continents, several countries and multi-cultural environments. She speaks and writes on disruptive technology convergence, innovation, tech ethics, cyber warfare, and national security.*

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 15 (28 Dec 17)

15. Battle of the Brain

In George Orwell's classic dystopian novel **1984**, O'Brien states,
"Power is in tearing human minds to pieces and putting them together again in new shapes of your own choosing."

Advances in Neuroscience and technology (NeuroS/T) are bringing this capability to the brink of reality. The Future Operational Environment (OE) will not be limited to conflict in the land, sea, air, cyber, and space domains. Direct attacks upon, and the manipulation of, Soldiers' and noncombatants' brains represent a significant threat, challenge, and opportunity in neurotechnology. The human brain will be a specific target of Multi Domain Battle.

At the Visualizing Multi Domain Battle 2030-2050 Conference, Georgetown University, 25-26 July 2017, Dr. James Giordano, Chief of the Neuroethics Program at Georgetown University, explained how neuroscience has made huge leaps by using technology to study and understand how the nervous system is structured and functions. NeuroS/T puts the brain at our fingertips, enabling us to better understand it.

This knowledge provides the potential for new and exciting ways to improve our memories, expand our cognitive abilities, and even repair damaged brains; conversely, it also presents new vulnerabilities that technologies can target and exploit.

For operators/warfighters, these include a number of "weapons" of choice that facilitate neuro-enablement:

• Advanced neuro-psychopharmacologics

•

Computational brain-machine interfaces

• Closed-loop brain stimulation approaches

• Neuro-sensory augmentation devices

While they are not traditional weapons like guns, missiles, or blades, these technologies will make warfighters more lethal, aware, resilient, and integrated with their combat systems.

On a darker note, novel neuroweapons will grant adversaries (and perhaps the United States) the ability to kill, disrupt, degrade, damage, and even “hack” human brains to influence populations, bring about confusion and panic, and disrupt an enemy’s government and society, often without mass casualties. As such, they constitute avenues of attack against the human brain, facilitating personalized warfare**. Neuroweapons are “Weapons of Mass Disruption” that may characterize major segments of warfare in the future.**

NeuroS/T provides a number of novel neuroweapons, including:

• Pharmaceuticals and organic neurotoxins (i.e., ultra-low dose/high specify agents for use in targeting diplomatic/local culture “hearts and minds” scenarios)

• High morbidity neuro-microbiologic agents (i.e., neuro-microbials with high neuro-psychiatric symptom clusters for public panic/public health disintegrative effects)

• Gene-edited microbiologicals with novel morbidity/mortality profiles

• Nano-neuroparticulate agents: high central nervous system (CNS) aggregation lead/carbon-silicate nanofibers (network disrupters); neurovascular hemorrhagic agents (for in-close and population use as “stroke epidemic” induction agents).

These capabilities afforded by neuroweapons and NeuroS/T bring with them a host of ethical and moral considerations and conundrums. We must address whether affecting someone’s brain purposely, even temporarily, violates ethical codes, treaties, conventions, and international norms followed by the United States military.

• Does current policy adequately address the roles and responsibilities of commanders and individual soldiers in their employment of such weapons?

• If you influence or impact human brains without causing death or physical pain, is this still an act of war or belligerence?

• How do we ensure our warfighters maintain a robust defense against and remain resilient in the face of neuro threats?

What is clear is that the United States must explore not only what is possible, but what is justified, appropriate, and legally possible in the Battle of the Brain.

For more information on this topic, please see the following presentations by Dr. Giordano:

• Neurotechnology in National Security and Defense, from this past summer’s Georgetown University Conference
• Neuroscience and the Weapons of War podcast, with Mr. John Amble, on Modern War Institute (MWI), 02 Aug 17

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 78 (23 August 18)

78. The Classified Mind – The Cyber Pearl Harbor of 2034

[**Editor's Note:** Mad Scientist Laboratory is pleased to publish the following post by guest blogger **Dr. Jan Kallberg**, faculty member, United States Military Academy at West Point, and Research Scientist with the Army Cyber Institute at West Point. His post serves as a cautionary tale regarding our finite intellectual resources and the associated existential threat in failing to protect them!]

Preface: Based on my experience in cybersecurity, migrating to a broader cyber field, there have always been those exceptional individuals that have an unreplicable ability to see the challenge early on, create a technical solution, and know how to play it in the right order for maximum impact. They are out there – the Einsteins, Oppenheimers, and Fermis of cyber. The arrival of Artificial Intelligence increases our reliance on these highly capable individuals – because someone must set the rules, the boundaries, and point out the trajectory for Artificial Intelligence at initiation.

As an industrialist society, we tend to see technology and the information that feeds it as the weapons – and ignore the few humans that have a large-scale direct impact. Even if identified as a weapon, how do you make a human mind classified? Can we protect these high-ability individuals that in the digital world are weapons, not as tools but compilers of capability, or are we still focused on the tools? Why do we see only weapons that are steel and electronics and not the weaponized mind as a weapon? I believe firmly that we underestimate the importance of **Applicable Intelligence** – the ability to play the cyber engagement in the optimal order. Adversaries are often good observers because they are scouting for our weak spots. I set the stage for the following post in 2034, close enough to be realistic and far enough for things to happen when our adversaries are betting that we rely more on a few minds than we are willing to accept.

Post: In a not too distant future, 20th of August 2034, a peer adversary's first strategic moves are the targeted killings of less than twenty individuals as they go about their daily lives: watching a 3-D printer making a protein sandwich at a breakfast restaurant; stepping out from the downtown Chicago monorail; or taking a taste of a poison-filled retro Jolt Cola. In the gray zone, when the geopolitical temperature increases, but we are still not at war yet, our adversary acts quickly and expedites a limited number of targeted killings within the United States of persons whom are unknown to mass media, the general public, and have only one thing in common – Applicable Intelligence (AI).

The ability to apply is a far greater asset than the technology itself. Cyber and card games have one thing in common, the order you play your cards matters. In cyber, the tools are publicly available, anyone can download them from the Internet and use them, but the weaponization of the tools occurs when used by someone who understands how to play the tools in an optimal order. These minds are different because they see an opportunity to exploit in a digital fog of war where others don't or can't see it. They address problems unburdened by traditional thinking, in new innovative ways, maximizing the dual-purpose of digital tools, and can create tangible cyber effects.

It is the Applicable Intelligence (AI) that creates the procedures, the application of tools, and turns simple digital software in sets or combinations as a convergence to digitally lethal weapons. This AI is the intelligence to mix, match, tweak, and arrange dual purpose software. In 2034, it is as if you had the supernatural ability to create a thermonuclear bomb from what you can find at Kroger or Albertson.

Sadly we missed it; we didn't see it. We never left the 20th century. Our adversary saw it clearly and at the dawn of conflict killed off the **weaponized minds**, without discretion, and with no concern for international law or morality.

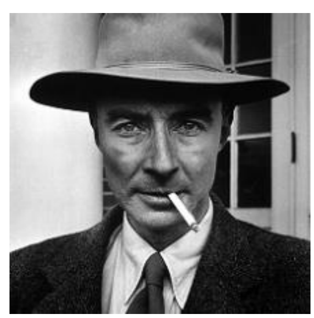
These intellects are **weapons of growing strategic magnitude.** In 2034, the United States missed the importance of these few intellects. This error left them unprotected.

All of our efforts were instead focusing on what they delivered, the application and the technology, which was hidden in secret vaults and only discussed in sensitive compartmented information facilities. Therefore, we classify to the highest level to ensure the confidentiality and integrity of our cyber capabilities. Meanwhile, the most critical component, the **militarized intellect**, we put no value to because it is a human. In a society marinated in an engineering mindset, humans are like desk space, electricity, and broadband; it is a commodity that is input in the production of the technical machinery. The marveled technical machinery is the only thing we care about today, 2018, and as it turned out in 2034 as well.

We are stuck in how we think, and we are unable to see it coming, but our adversaries see it. At a systematic level, we are unable to see humans as the weapon itself, maybe because we like to see weapons as something tangible, painted black, tan, or green, that can be stored and brought to action when needed. As the armory of the war of 1812, as the stockpile of 1943, and as the launch pad of 2034. Arms are made of steel, or fancier metals, with electronics – we failed in 2034 to see weapons made of corn, steak, and an added combative intellect.

General Nakasone stated in 2017, “Our best ones [coders] are 50 or 100 times better than their peers,” and continued “Is there a sniper or is there a pilot or is there a submarine driver or anyone else in the military 50 times their peer? I would tell you, some coders we have are 50 times their peers.” In reality, the success of cyber and cyber operations is highly dependent not on the tools or toolsets but instead upon the **super-empowered individual** that General Nakasone calls “the 50-x coder.”

There were clear signals that we could have noticed before General Nakasone pointed it out clearly in 2017. The United States’ Manhattan Project during World War II had at its peak 125,000 workers on the payroll, but the intellects that drove the project to success and completion were few. The difference with the Manhattan Project and the future of cyber is that we were unable to see the human as a



weapon, being locked in by our path dependency as an engineering society where we hail the technology and forget the importance of the humans behind it.

America's endless love of technical innovations and advanced machinery reflects in a nation that has celebrated mechanical wonders and engineered solutions since its creation. For America, technical wonders are a sign of prosperity, ability, self-determination, and advancement, a story that started in the early days of the colonies, followed by the intercontinental railroad, the Panama Canal, the manufacturing era, the moon landing, and all the way to the autonomous systems, drones, and robots. In a default mindset, there is always a tool, an automated process, a software, or a set of technical steps that can solve a problem or act.

The same mindset sees humans merely as an input to technology, so humans are interchangeable and can be replaced. In 2034, the era of digital conflicts and the war between algorithms with engagements occurring at machine speed with no time for leadership or human interaction, it is the intellects that design and understand how to play it. We didn't see it.

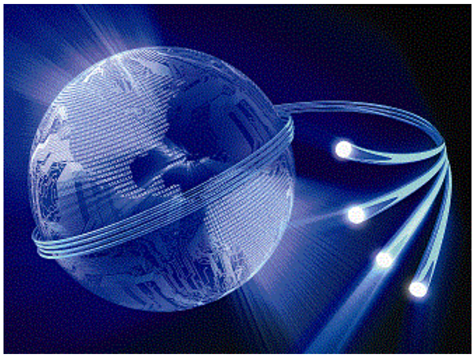
In 2034, with fewer than twenty bodies piled up after targeted killings, resides the Cyber Pearl Harbor. It was not imploding critical infrastructure, a tsunami of cyber attacks, nor hackers flooding our financial systems, but instead traditional lead and gunpowder. The super-empowered individuals are gone, and we are stuck in a digital war at speeds we don't understand, unable to play it in the right order, and with limited intellectual torque to see through the fog of war provided by an exploding kaleidoscope of nodes and digital engagements.

If you enjoyed this post, read our Personalized Warfare post.

Dr. Jan Kallberg *is currently an Assistant Professor of Political Science with the Department of Social Sciences, United States Military Academy at West Point, and a Research Scientist with the Army Cyber Institute at West Point. He was earlier a researcher with the Cyber Security Research and Education Institute, The University of Texas at Dallas, and is a part-time faculty member at George Washington University. Dr. Kallberg earned his Ph.D. and MA from the University of Texas at Dallas and earned a JD/LL.M. from Juridicum Law School, Stockholm University. Dr. Kallberg is a certified CISSP, ISACA CISM, and serves as the Managing Editor for the Cyber Defense Review. He has authored papers in the Strategic Studies Quarterly, Joint Forces Quarterly, IEEE IT Professional, IEEE Access, IEEE Security and Privacy, and IEEE Technology and Society.*

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 66 (09 July 18)



66. Virtual Nations: An Emerging Supranational Cyber Trend

[**Editor's Note:** Mad Scientist Laboratory is pleased to feature today's guest blog post by **Ms. Marie Murphy**, addressing the rise of Virtual Nations and the associated national security ramifications.]

The world is becoming increasingly digitized, and there is a rising threat from online organizations that could mimic and come to rival governments. These **virtual nations** are cyber communities which have succeeded in gaining power, influence, or capital comparable to that of a nation-state, posing a unique security threat that does not respond to traditional Army methodology and technology.

There are two broad categories of virtual nations. The first is when a nation-state digitizes all of its information and government services, potentially offering programs such as e-Residency. **Estonia** was the first digital nation and leads the pack in this technology. The second are virtual nations not supported by any government, existing only online, such as **Asgardia**, which recently launched a nanosatellite into orbit containing its citizens' data[i]. These organizations are called nations by virtue of sign-up based "citizenship" and a political or **ideological allegiance**. Both categories rely on blockchain technology to maintain their operations[ii].

The latter category possesses the greater threat potential towards the US and its military. By 2050, as certain ideologically based online communities become more prolific and organized, members may begin to feel a stronger attachment and sense of belonging to their online identity than to their nationality[iii]. Once virtual nations are large enough to have power and control over the beliefs and actions of their citizens, they may begin to demand **official recognition**. They would already possess internal recognition: everyone within the nation believing that it is a nation. The second type of recognition, external, is granted through recognition by an outside body[iv] and signifies its legitimacy (which can take multiple forms, from terrorist organization all the way to governing entity).

It is highly unlikely that virtual nations will be officially recognized by 2050. If this becomes the case in the far distant future, the US Army is bound by its own doctrine and rules of engagement, as well as by international law and UN convention. This is the preferable scenario because it allows the Army to follow the combat and operation rules with which it is already familiar.

As of now, there is no official recognition for virtual nations. This makes virtual nations more dangerous because there is no external accountability or regulation. The idea of virtual nations will grow in popularity as some people become disenfranchised with their state government and search in larger numbers for organizations of other like-minded people online. Negotiation and diplomacy may not be options with virtual nations, enabling and possibly incentivizing sudden and unilateral action.

Rome wasn't built in a day, and neither was the modern nation-state, which will not be quickly supplanted. However, the political power of the nation-state will start to decline as virtual nations begin to offer comparable services and security. Legitimate government actions may blend in with those of individuals and non-state actors in a haze of **anonymity**[v]. Given that virtual nations are not yet prolific enough to have a significant impact on operations and global society, there are several key questions that the Army should begin to examine now, ranging from operational to legal and moral:

- How can the Army modernize to defend against attacks not only from isolated cyber groups or nation-state supported hacking efforts, but from massive online organizations with widely distributed membership?

• What happens when the plurality of people belong to virtual nations and they value their doctrine above that of their nation-state?

• What is the protocol if cyber war extends to the physical or conventional domain?

• Can the US Army legally and ethically conduct targeted cyber or physical strikes against civilians who are involved in a cyber-attack or acts of cyber warfare? If so, who is targeted if the attack comes from multiple different dispersed systems?

• Are the people behind the computer screen writing malicious code viewed as combatants?

Considering this plethora of unknowns, there are some steps that the Army can take today and in the future to prepare for the rise of this new type of organization:

There is a need to update Army doctrine addressing how the Army would engage in **cyber war** against a virtual nation or similar organization[vi]. Such a conflict will involve consistent and coordinated efforts from participants in multiple countries without state affiliation. These nations can amass support and launch or counter actions much quicker than the Army is used to, and the lack of adversary proximity presents a logistical and operational challenge for the Army. Doctrinal changes made in 2013 continued to emphasize human capabilities after a decade of intensive COIN (counter-insurgency) operations. However, there is still a **gap in understanding** how CEMA (cyber-electromagnetic activities) and IO (information operations) should work together in synchronicity to fight virtual threats[vii]. Closing this gap would bring the Army one step closer to optimally operating in the digital domain and effectively using all of the tools at its disposal.

The Army should also continue expanding its cyber force, investing in drones (which could drop small payloads on servers that facilitate attacks or acts of cyber warfare), and making improvements on technologies that can decrypt and trace online accounts to their owners. The Army will also need an updated database of potentially hostile virtual nations and their capabilities. These future capabilities will require closer interactions with the Intelligence Community (IC).

The future may bring a world where a person's identity is not based on their geography but on their, political, entrepreneurial, or ideological subscriptions. The Army will not just combat government-sponsored or fringe hacking groups in 2050. These virtual nations pose a unique threat to the US because they are not deterred or combatted through traditional doctrine and tactics.

Special recognition belongs to USAF Lt. Col. Jennifer "JJ" Snow for her inspiring research and writing on this topic.

Marie Murphy *is a rising junior at The College of William and Mary in Virginia, studying International Relations and Arabic. She is currently interning at Headquarters, US Army Training and Doctrine Command (TRADOC) with the Mad Scientist Initiative.*

---

[i] "**Asgardia, the World's First 'Virtual Space Nation'**," The Week, 20 Nov. 2017.

[ii] "**The Nation State Goes Virtual**," Nesta, 2018.

[iii], Frey, Thomas, Juan F "Kiko" Suarez, and Eduardo Suarez, "**The Virtual Country: Six Possible Scenarios for the Creation of Viable Virtual Countries**," The Wirtland Institute, n.d.

[iv] Ibid.

[v] Wagner, Daniel, "**In the Era of Virtual Terrorism, All Cyber-Enabled Nations are Equal**," International Policy Digest, 20 Nov 2017.

[vi] Banach, Stefan J, "**Virtual War and Weapons of Mass Deception**," Modern War Institute, 19 April 2018.

[vii] Sheiffer, Matthew J, Lt. Col. "**U.S. Army Information Operations and Cyber-Electromagnetic Activities: Lessons from Atlantic Resolve**," Army University Press, 19 March 2018.

Return to the Table of Contents

Chapter 5. Conference Findings

Return to the Table of Contents

This page intentionally left blank

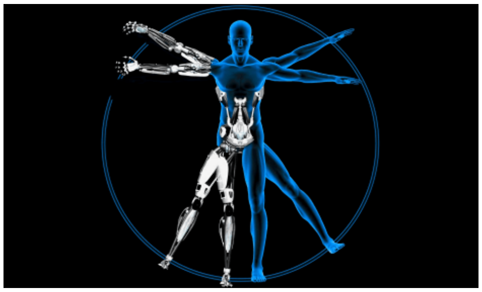
Mad Scientist Laboratory Blog Post 68 (16 July 18)

67. Bio Convergence and Soldier 2050 Conference Final Report

[**Editor's Note:** The U.S. Army Training and Doctrine Command (TRADOC) co-hosted the **Mad Scientist Bio Convergence and Soldier 2050 Conference** with SRI International on 8–9 March 2018 at their Menlo Park campus in California. This conference explored bio convergence, what the Army's Soldier of 2050 will look like, and how they will interact and integrate with their equipment. The following post is an excerpt from this conference's final report.]

While the technology and concepts defining warfare have continuously and rapidly transformed, the primary actor in warfare – the human – has remained largely unchanged. Soldiers today may be physically larger, more thoroughly trained, and better equipped than their historical counterparts, but their capability and performance abilities remain very similar.

These limitations in human performance, however, may change over the next 30 years, as advances in biotechnology and human performance likely will expand the boundaries of what is possible for humans to achieve. We may see Soldiers – not just their equipment – with superior vision, enhanced cognitive abilities, disease/virus resistance, and increased strength, speed, agility, and endurance. As a result, these advances could provide the Soldier with an edge to survive and thrive on the hyperactive, constantly changing, and increasingly lethal **Multi-Domain Battlespace**.



In addition to potentially changing the individual physiology and abilities of the future Soldier, there are many technological innovations on the horizon that will impact human performance. The convergence of these technologies – **artificial intelligence (AI)**, **robotics**, **augmented reality**, **brain-machine interface**, nanotechnologies, and biological and medical improvements to the human – is referred to as **bio convergence**. Soldiers of the future will have enhanced capabilities due to technologies that will be installed, instilled, and augmented. This convergence will also make the Army come to terms on what kinds of bio-converged technologies will be accepted in **new recruits**.

The conference generated the following key findings:

• The broad advancement of biotechnologies will provide wide access to dangerous and powerful bioweapons and human enhancements. The low cost and low expertise entry point into gene editing, human performance enhancement, and bioweapon production has spurred a string of new explorations into this arena by countries with large defense budgets (e.g., China), non-state criminal and terrorist organizations (e.g., ISIS), and even **super-empowered individuals** willing to subject their bodies to experimental and risky treatments.

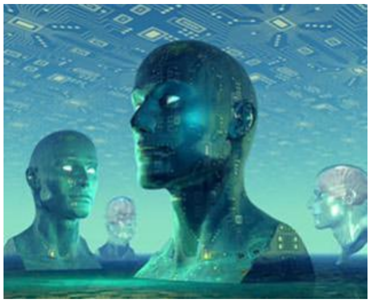
• Emerging synthetic biology tools (e.g., CRISPR, Talon, and ZFN) present an opportunity to engineer Soldiers' DNA and enhance their performance, providing greater speed, strength, endurance, and resilience. These tools, however, will also create new vulnerabilities, such as **genomic targeting**, that can be exploited by an adversary and/or potentially harm the individual undergoing enhancement. Bioengineering is becoming easier and cheaper as a bevy of developments are reducing biotechnology transaction costs in gene reading, writing, and editing. Due to the ever-increasing speed and lethality of the **future battlefield**, combatants will need cognitive and physical enhancement to survive and thrive.

• Ensuring that our land forces are ready to meet future challenges requires optimizing biotechnology and neuroscience advancements. Designer viruses and diseases will be highly volatile, mutative, and extremely personalized, potentially challenging an already stressed Army medical response system and its countermeasures. Synthetic biology provides numerous **applications** that will bridge capability gaps and enable future forces to fight effectively. Future synthetic biology defense applications are numerous and range from sensing capabilities to rapidly developed vaccines and therapeutics.

• Private industry and academia have become the driving force behind innovation. While there are some benefits to this – such as shorter development times – there are also risks. For example, investments in industry are mainly driven by market demand which can lead to a lack of investment in areas that are vital to National Defense but have low to no consumer demand. In academia, a majority of graduate students in STEM fields are foreign nationals, comprising over 80% of electrical and petroleum engineering programs. The U.S. will need to find a way to maintain its technological superiority even when most of the expertise eventually leaves the country.

• The advent of new biotechnologies will give rise to moral, regulatory, and legal challenges for the Army of the Future, its business practices, recruiting requirements, Soldier standards, and structure. The rate of technology development in the synthetic biology field is increasing rapidly. Private individuals or small start-ups with minimal capital can create a new organism for which there is no current countermeasure and the development of one will likely take years. This potentiality leads to the dilemma of swiftly creating effective policy and regulation that addresses these concerns, while not stifling creativity and productivity in the field for those conducting legitimate research. Current regulation **may not be sufficient**, and bureaucratic inflexibility prevents quick reactive and proactive change. Our adversaries may not move as readily to adopt harsher regulations in the bio-technology arena. Rather than focusing on short-term solutions, it may be beneficial to take a holistic approach centered in a world where bio-technology is interacting with everyday life. The U.S. may have to work from a relative “disadvantage,” using safe and legal methods of enhancement, while our adversaries may choose to operate below our defined legal threshold.

Bio Convergence is incredibly important to the Army of the Future because the future Soldier ***is*** the Bio. The Warrior of tomorrow’s Army will be given more responsibility, will be asked to do more, will be required to be more capable, and will face more challenges and complexities than ever before. These Soldiers must be able to quickly adapt, change, connect to and disconnect from a multitude of networks – digital and otherwise – all while carrying out multiple mission-sets in an increasingly disrupted, degraded, and arduous environment marred with distorted reality, information warfare, and attacks of a personalized nature.



For additional information regarding this conference:

• Review the **Lessons Learned from the Bio Convergence and Soldier 2050 Conference** preliminary assessment.

• Read the entire **Mad Scientist Bio Convergence and Soldier 2050 Conference Final Report**.

• Watch the conference’s **video presentations**.

• See the associated presentations’ **briefing slides**.

• Check out the associated “Call for Ideas” writing contest **finalist submissions**, hosted by our colleagues at ***Small Wars Journal***.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 52 (14 May 18)

51. Black Swans and Pink Flamingos

The **Mad Scientist Initiative** recently facilitated a workshop with thought leaders from across the Department of Defense, the Intelligence Community, other Government agencies, industry, and academia to address the **unknown, unknowns** (i.e., Black Swans) and the **known, knowns** (i.e., Pink Flamingos) to **synthesize cross-agency thinking** about possible **disruptions** to the **Future Operational Environment**.

Black Swans: In **Nassim Nicholas Taleb**'s original context, a black swan (unknown, unknowns) is an event or situation which is **unpredictable**, but has a **major effect**. For this conference, we used a looser definition, identifying possibilities that are **not likely**, but might have **significant impacts** on how we think about **warfighting** and **security**.

Pink Flamingos: Defined by **Frank Hoffman**, Pink Flamingos are the known, knowns that are **often discussed, but ignored** by Leaders trapped by **organizational cultures** and rigid **bureaucratic decision-making structures**. **Peter Schwartz** further describes Pink Flamingos as the "**inevitable surprise**." Digital photography was a pink flamingo to **Kodak**.

At the workshop, attendees identified the following **Black Swans**:

• **Naturally Occurring Disaster:** These events (i.e., Carrington Event — solar flare frying solid state electronics, super volcano eruptions, earthquake swarms, etc.) would have an **enormous impact** on the Army and its ability to continue to **operate** and **defend** the nation and **support national recovery operations**. While warning times have increased for many of these events, there are **limited measures** that can be implemented to mitigate the **devastating effects** of these events.

• **Virtual Nations:** While the **primacy** of **Westphalian borders** has been **challenged** and the power of **traditional nation-states** has been **waning** over the last decade, some political scientists have assumed that **supranational organizations** and **non-state actors** would take their place. One potential black swan is the emergence of **virtual nations** due to the convergence of **blockchain technologies**, **crypto-currency,** and the ability to **project power** and **legitimacy** through the **virtual world**. Virtual nations could be organized based on **ideologies, business models,** or **single interests**. Virtual nations could **supersede, supplement,** or **compete** with **traditional, physical nations**. The Army of the future may not be prepared to **interact** and **compete with virtual nations**.

• **Competition in Venues Other than Warfare (Economic, Technological, Demographic, etc.) Achieving Primacy:** In the near future, war in the traditional sense may be **less prevalent**, while **competitions in other areas** may be the driving forces behind national oppositions. How does the Army need to prepare for an eventuality where **armed conflict** is **not as important** as it once was?

• **Alternate Internet — “Alternet”:** A **distinct entity**, separate from the general commercial internet, **only accessible** with **specific corresponding hardware**. This technology would allow for **unregulated and unmonitored communication** and **commerce**, potentially granting safe haven to **criminal** and **terrorist activities**.

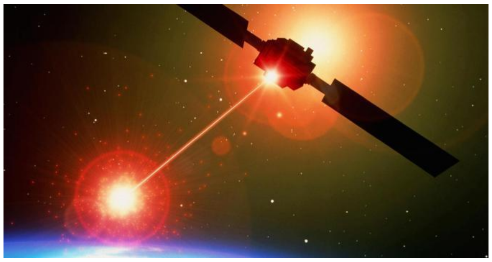
At the workshop, attendees identified the following **Pink Flamingos**:

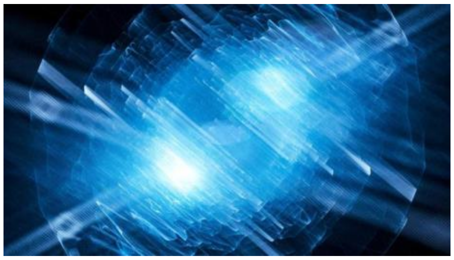
• **Safe at Home:** Army installations are **no longer** the **sanctuaries** they once were, as adversaries will be able to **attack Soldiers** and **families** through **social media** and other **cyberspace means**. Additionally, installations no longer merely house, train, and deploy Soldiers — **unmanned combat systems** are controlled from home installations -— a trend in virtual power that will increase in the future. The Army needs a plan to **harden** our **installations** and **train Soldiers** and **families** to be resilient for this eventuality.

• **Hypersonics:** High speed (**Mach 5** or higher) and **highly maneuverable** missiles or glide vehicles that can **defeat** our **air defense systems**. The **speed** of these weapons is **unmatched** and their **maneuverability** allows them to keep their targets unknown until only seconds before impact, negating **current countermeasures**.

• **Generalized, Operationalized Artificial Intelligence (AI):** **Artificial intelligence** is one of the most prominent pink flamingos throughout global media and governments. Narrow artificial intelligence is being addressed as rapidly as possible through ventures such as **Project MAVEN**. However, generalized and operationalized artificial intelligence – that can think, contextualize, and operate like a human – has the potential to **disrupt** not only **operations**, but also the **military** at its **very core** and **foundation**.

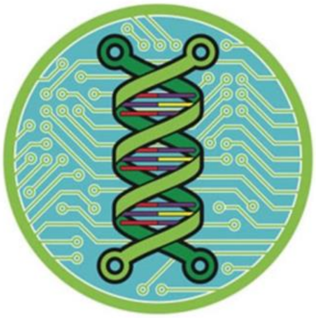
• **Space/Counterspace:** Space is becoming increasingly congested, commercialized, and democratized. **Disruption, degradation,** and **denial** in space threatens to **cripple multi-domain warfare operations**. States and non-state actors alike are exploring options to **counter** one another, **compete,** and potentially **even fight in space**.

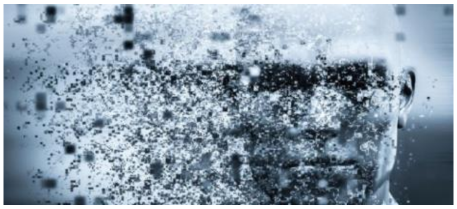




• **Quantum Sciences:** Quantum science – communication, computing, and sensing – has the potential to solve some intractable but very specific problem sets. **Quantum technology** remains in its infancy. However, as the growth of **qubits** in **quantum computing** continues to expand, so does the potentiality of traditional encryption being utterly broken. **Quantum sensing** can allow for much more precise atomic clocks surpassing the precision timing of GPS, as well as **quantum imaging** that provides **better results** than classical imaging in a variety of wavelengths.

• **Bioweapons/Biohacking:** The democratization of **bio technology** will mean that **super-empowered individuals** as well as nation states will have the ability to **engineer weapons** and **hacks** that can augment friendly human forces or target and degrade enemy human forces (e.g., targeted disease or genetic modifications).





• **Personalized Warfare:** Warfare is now waged on a **personal** level, where adversaries can **attack** the bank accounts of Soldiers' families, **infiltrate** their social media, or even **target** them specifically by their genetics. The Army needs to understand that the **individual Soldier** can be **exploited** in many different ways, **often through information** publicly provided or stolen.

• **Deep Fakes/Information Warfare:** Information warfare and "fake news" have played a **prominent role** in **global politics** over the last several years and could **dominate** the relationship between societies, governments, politicians, and militaries in the future operational environment. **Information operations**, thanks to big data and humanity's ever-growing digital presence, are targeted at an **extremely personal** and **specific level**. One of the more concerning aspects of this is an artificial intelligence-based human image/voice synthesis technique known as **deep fakes**. Deep fakes can essentially **put words** in the **mouths** of prominent or trusted politicians and celebrities.

• **Multi-Domain Swarming:** Swarming is often thought about in terms of unmanned aerial systems (UAS), but one significant pink flamingo is swarming taking place across **multiple domains** with **self-organizing, autonomous aerial, ground, maritime (sub and surface),** and even **subterranean unmanned systems**. U.S. defense systems on a linear modernization and development model will not be capable of dealing with the **saturation** and **complexity issues** arising from these multi-domain swarms.

• **Lethal Autonomy:** An **autonomous system** with the ability to track, target, and fire without the supervision or authority of a **human in/on the loop**. The U.S. Army will have to examine its own policy regarding these issues as well as our adversaries, who may be less deterred by **ethical/policy issues**.

• **Tactical Nuclear Exchange:** While **strategic nuclear war** and **mutually assured destruction** have been discussed and addressed *ad nauseam*, not enough attention has been given to the potential of a tactical nuclear exchange between state actors. One tactical nuclear attack, while not guaranteeing a nuclear holocaust, would bring about a myriad of problems for U.S. forces worldwide (e.g., the potential for **escalation, fallout, contamination** of water and air, and **disaster response**). Additionally, a high altitude nuclear burst's **electromagnetic pulse** has the potential to fry solid state electronics across a wide-area, with **devastating results** to the affected nation's **electrical grid, essential government services,** and **food distribution networks**.

Leaders must anticipate these **future possibilities** in determining the character of future conflicts and in force design and equipping decisions. Using a mental model of **black swans** and **pink flamingos** provides a helpful framework for assessing the risks associated with these decisions.

For additional information on projected black swans for the next 20+ years, see the RAND Corporation's **Discontinuities and Distractions — Rethinking Security for the Year 2040**.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 64 (28 June 18)

64. Top Ten Takeaways from the Installations of the Future Conference

On 19-20 June 2018, the U.S. Army Training and Doctrine Command (TRADOC) Mad Scientist Initiative co-hosted the Installations of the Future Conference with the Office of the Assistant Secretary of the Army for Installations, Energy and Environment (OASA (IE&E)) and Georgia Tech Research Institute (GTRI). Emerging technologies supporting the hyper-connectivity revolution will enable improved training capabilities, security, readiness support (e.g., holistic medical facilities and brain gyms), and quality of life programs at Army installations. Our concepts and emerging doctrine for multi-domain operations recognizes this as increasingly important by including Army installations in the Strategic Support Area. Installations of the Future will serve as mission command platforms to project virtual power and expertise as well as Army formations directly to the battlefield.

We have identified the following "Top 10" takeaways related to our future installations:

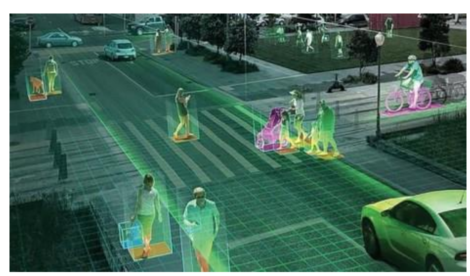
1. Threats and Tensions. "*Army Installations are no longer sanctuaries*" — Mr. Richard G. Kidd IV, Deputy Assistant Secretary of the Army, Strategic Integration. There is a tension between openness and security that will need balancing to take advantage of smart technologies at our Army installations. The revolution in connected devices and the ability to virtually project power and expertise will increase the potential for adversaries to target our installations. Hyper-connectivity increases the attack surface for cyber-attacks and the access to publicly available information on our Soldiers and their families, making **personalized warfare** and the use of **psychological attacks and deep fakes** likely.

2. Exclusion vs. Inclusion. The role of and access to future Army installations depends on the balance between these two extremes. The connections between local communities and Army installations will increase potential threat vectors, but resilience might depend on expanding inclusion. Additionally, access to specialized expertise in **robotics**, **autonomy**, and information technologies will require increased connections with outside-the-gate academic institutions and industry.

3. Infrastructure Sensorization. Increased sensorization of infrastructure runs the risk of driving efficiencies to the point of building in unforeseen risks. In the business world, these efficiencies are profit-driven, with clearer risks and rewards. Use of table top exercises can explore hidden risks and help Garrison Commanders to build resilient infrastructure and communities. Automation can cause **cascading failures** as people begin to fall "out of the loop."

4. Army Modernization Challenge. Installations of the Future is a microcosm of overarching Army Modernization challenges. We are simultaneously invested in legacy infrastructure that we need to upgrade, and making decisions to build new smart facilities. Striking an effective and efficient balance will start with public-private partnerships to capture the expertise that exists in our universities and in industry. The expertise needed to succeed in this modernization effort does not exist in the Army. There are significant opportunities for Army Installations to participate in ongoing consortiums like the "Middle Georgia" Smart City Community and the Global Cities Challenge to pilot innovations in spaces such as energy resilience.

5. Technology is outpacing regulations and policy. The sensorization and available edge analytics in our public space offers improved security but might be perceived as decreasing personal privacy. While we give up some personal privacy when we live and work on Army installations, this collection of data will require active engagement with our communities. We studied an ongoing Unmanned Aerial System (UAS) support **concept** to detect gunshot incidents in Louisville, KY, to determine the need to involve legislatures, local political leaders, communities, and multiple layers of law enforcement.



6. Synthetic Training Environment. The Installation of the Future offers the Army significant opportunities to divest itself of large brick and mortar training facilities and stove-piped, contractor support-intensive Training Aids, Devices, Simulations, and Simulators (TADSS). MG Maria Gervais, Deputy Commanding General, Combined Arms Center – Training (DCG, CAC-T), presented the Army's **Synthetic Training Environment (STE)**, incorporating **Virtual Reality (VR)**, "big box" open-architecture simulations using a One World Terrain database, and reduced infrastructure and contractor-support footprints to improve Learning and Training. The STE, delivering high-fidelity simulations and the opportunity for our Soldiers and Leaders to exercise all Warfighting Functions across the full Operational Environment with greater repetitions at home station, will complement the Live Training Environment and enhance overall Army readiness.

7. Security Technologies. Many of the security-oriented technologies (autonomous drones, camera integration, facial recognition, edge analytics, and **Artificial Intelligence**) that triage and fuse information will also improve our deployed Intelligence, Surveillance, and Reconnaissance (ISR) capabilities. The Chinese lead the world in these technologies today.

8. Virtual Prototyping. The U.S. Army Engineer Research and Development Center (ERDC) is developing a computational testbed using **virtual prototyping** to determine the best investments for future Army installations. The four drivers in planning for Future Installations are: 1) Initial Maneuver Platform (Force Projection); 2) Resilient Installations working with their community partners; 3) Warfighter Readiness; and 4) Cost effectiveness in terms of efficiency and sustainability.

9. Standard Approach to Smart Installations. A common suite of tools is needed to integrate smart technologies onto installations. While Garrison Commanders need mission command to take advantage of the specific cultures of their installations and surrounding communities, the Army cannot afford to have installations going in different directions on modernization efforts. A method is needed to rapidly pilot prototypes and then determine whether and how to scale the technologies across Army installations.

10. "Low Hanging Fruit." There are opportunities for Army Installations to lead their communities in tech integration. Partnerships in energy savings, waste management, and early 5G infrastructure provide the Army with early adopter opportunities for collaboration with local communities, states, and across the nation. We must educate contracting officers and Government consumers to look for and seize upon these opportunities.

Videos from each of the Installations of the Future Conference presentations are posted **here**. The associated slides will be posted **here** within the week on the Mad Scientist All Partners Access Network site.

If you enjoyed this post, check out the following:

• Watch Mr. Richard Kidd IV discuss Installations of the Future on **Government Matters**.

• Read Mad Scientist Ed Blayney's takeaways from the Installations of the Future Conference in his article, entitled **We need more Mad Scientists in our Smart Cities**.

• See the TRADOC G-2 Operational Environment Enterprise's:

   – **The Changing Character of Future Warfare** video.

   – **Evolving Threats to Army Installations** video.

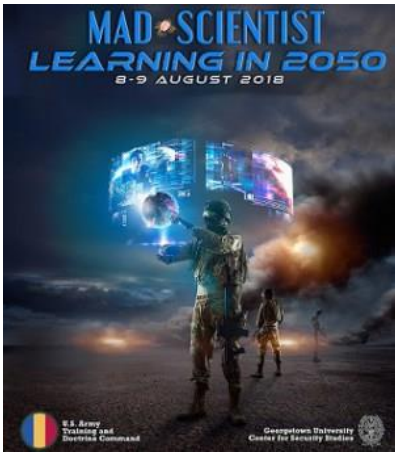
• Review our Call for Ideas winning submissions **Trusting Smart Cities: Risk Factors and Implications** by Dr. Margaret Loper, and **Day in the Life of a Garrison Commander** by the team at AT&T Global Public Sector — both are graciously hosted by our colleagues at ***Small Wars Journal***.

• Re-visit our following blog posts: **Smart Cities and Installations of the Future: Challenges and Opportunities** and **Base in a Box**.

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 76 (16 August 18)

76. Top Ten Takeaways from the Learning in 2050 Conference



On 8-9 August 2018, the U.S. Army Training and Doctrine Command (TRADOC) co-hosted the **Learning in 2050 Conference** with Georgetown University's Center for Security Studies in Washington, DC. Leading scientists, innovators, and scholars from academia, industry, and the government gathered to address future learning techniques and technologies that are critical in preparing for Army operations in the mid-21st century against adversaries in rapidly evolving battlespaces. The new and innovative learning capabilities addressed at this conference will enable our Soldiers and Leaders to act quickly and decisively in a changing Operational Environment (OE) with fleeting windows of opportunity and more advanced and lethal technologies.

We have identified the following "Top 10" takeaways related to Learning in 2050:

1. Many learning technologies built around commercial products are available today (Amazon Alexa, Smart Phones, Immersion tech, Avatar experts) for introduction into our training and educational institutions. Many of these technologies are part of the Army's concept for a **Synthetic Training Environment (STE)** and there are nascent manifestations already. For these technologies to be widely available to the future Army, the Army of today must be prepared to address:

– The **collection and exploitation** of as much data as possible;

– The policy concerns with security and privacy;

– The cultural challenges associated with **changing the dynamic** between learners and instructors, teachers, and coaches; and

– The adequate funding to produce capabilities at scale so that digital tutors or other technologies (**Augmented Reality [AR] / Virtual Reality [VR]**, etc.) and skills required in a dynamic future, like critical thinking/group think mitigation, are widely available or perhaps ubiquitous.

2. Personalization and individualization of learning in the future will be paramount, and some training that today takes place in physical schools will be more the exception, with learning occurring at the point of need. This transformation will not be limited to lesson plans or even just learning styles:

– **Intelligent tutors**, **Artificial Intelligence (AI)**-driven instruction, and targeted mentoring/tutoring;

– Tailored timing and pacing of learning (when, where, and for what duration best suits the individual learner or group of learners?);

– Collaborative learners will be teams partnering to learn;

– Various media and technologies that enable enhanced or accelerated learning (**Targeted Neuroplasticity Training (TNT)**, **haptic sensors**, AR/VR, **lifelong personal digital learning partners**, pharmaceuticals, etc.) at scale;

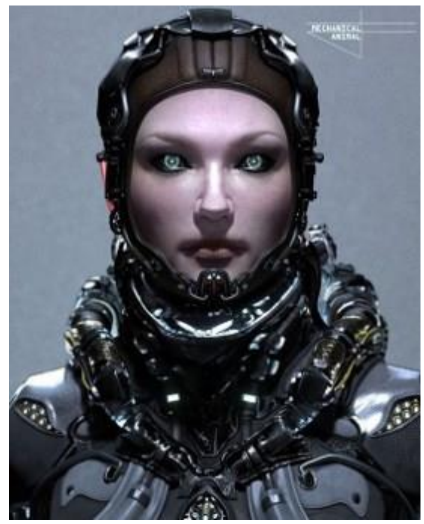
– Project-oriented learning; when today's high school students are building apps, they are asked "What positive change do you want to have?" One example is an open table for Bully Free Tables. In the future, learners will learn through working on projects;

– Project-oriented learning will lead to a convergence of learning and operations, creating a chicken (learning) or the egg (mission/project) relationship; and

– Learning must be adapted to consciously address the desired, or extant, culture.

3. Some jobs and skill sets have not even been articulated yet. Hobbies and recreational activities engaged in by kids and enthusiasts today could become occupations or Military Occupational Specialties (MOS's) of the future (e.g., drone creator/maintainer, 3-D printing specialist, digital and cyber fortification construction engineer — think **Minecraft** and **Fortnite** with real-world physical implications). Some emerging trends in **personalized warfare**, big data, and **virtual nations** could bring about the necessity for more specialists that don't currently exist (e.g., data protection and/or data erasure specialists).

4. The New Human (who will be born in 2032 and is the recruit of 2050) will be fundamentally different from the Old Human. The Chief of Staff of the Army (CSA) in 2050 is currently a young Captain in our Army today. While we are arguably cyborgs today (with integrated electronics in our pockets and on our wrists), the New Humans will likely be cyborgs in the truest sense of the word, with some having **embedded sensors**. How will those New Humans learn? What will they need to learn? Why would they want to learn something? These are all critical questions the Army will continue to ask over the next several decades.



5. Learning is continuous and self-initiated, while education is a point in time and is "done to you" by someone else. Learning may result in a certificate or degree – similar to education – or can lead to the foundations of a skill or a deeper understanding of operations and activity. How will organizations quantify learning in the future? Will degrees or even certifications still be the benchmark for talent and capability?

6. Learning isn't slowing down, it's speeding up. More and more things are becoming instantaneous and humans have no concept of **extreme speed**. Tesla cars have the ability to update software, with owners getting into a veritably different car each day. What happens to our Soldiers when military vehicles change much more iteratively? This may force a paradigm shift wherein learning means tightening local and global connections (tough to do considering government/military network securities, firewalls, vulnerabilities, and constraints); viewing technology as extended brains all networked together (similar to **Dr. Alexander Kott**'s look at the Internet of Battlefield Things [IoBT]); and leveraging these capabilities to enable Soldier learning at extremely high speeds.

7. While there are a number of emerging concepts and technologies to improve and accelerate learning (TNT, extended reality, personalized learning models, and intelligent tutors), the focus, training stimuli, data sets, and desired outcomes all have to be properly tuned and aligned or the Learner could end up losing correct behavior habits (developing maladaptive plasticity), developing incorrect or skewed behaviors (per the desired capability), or assuming inert cognitive biases.

8. Geolocation may become increasingly less important when it comes to learning in the future. If Apple required users to go to Silicon Valley to get trained on an iPhone, they would be exponentially less successful. But this is how the Army currently trains. The ubiquity of connectivity, the growth of the Internet of Things (and eventually Internet of Everything), the introduction of universal interfaces (think one XBOX controller capable of controlling 10 different types of vehicles), major advances in modeling and simulations, and social media innovation all converge to minimize the importance of teachers, students, mentors, and learners being collocated at the same physical location.

9. Significant questions have to be asked regarding the specificity of training in children at a young age to the point that we may be overemphasizing STEM from an early age and not helping them learn across a wider spectrum. We need **Transdisciplinarity** in the coming generations.

10. 3-D reconstructions of bases, training areas, cities, and military objectives coupled with mixed reality, haptic sensing, and intuitive controls have the potential to dramatically change how Soldiers train and learn when it comes to not only single performance tasks (e.g., marksmanship, vehicle driving, reconnaissance, etc.) but also in dense urban operations, multi-unit maneuver, and command and control.

During the next two weeks, we will be posting the videos from each of the **Learning in 2050 Conference** presentations on the TRADOC G-2 Operational Environment (OE) Enterprise **YouTube Channel** and the associated slides on our Mad Scientist **APAN site** — stay connected here at the Mad Scientist Laboratory.

One of the main thrusts in the Mad Scientist lines of effort is harnessing and cultivating the Intellect of the Nation. In this vein, we are asking **Learning in 2050 Conference** participants (both in person and online) to share their ideas on the presentations and topic. Please consider:

– What topics were most important to you personally and professionally?

– What were your main takeaways from the event?

– What topics did you want the speakers to extrapolate more on?

– What were the implications for your given occupation/career field from the findings of the event?

Your input will be of critical importance to our analysis and products that will have significant impact on the future of the force in design, structuring, planning, and training! Please submit your input to Mad Scientist at: **usarmy.jble.tradoc.mbx.army-mad-scientist@mail.mil**.

Return to the Table of Contents