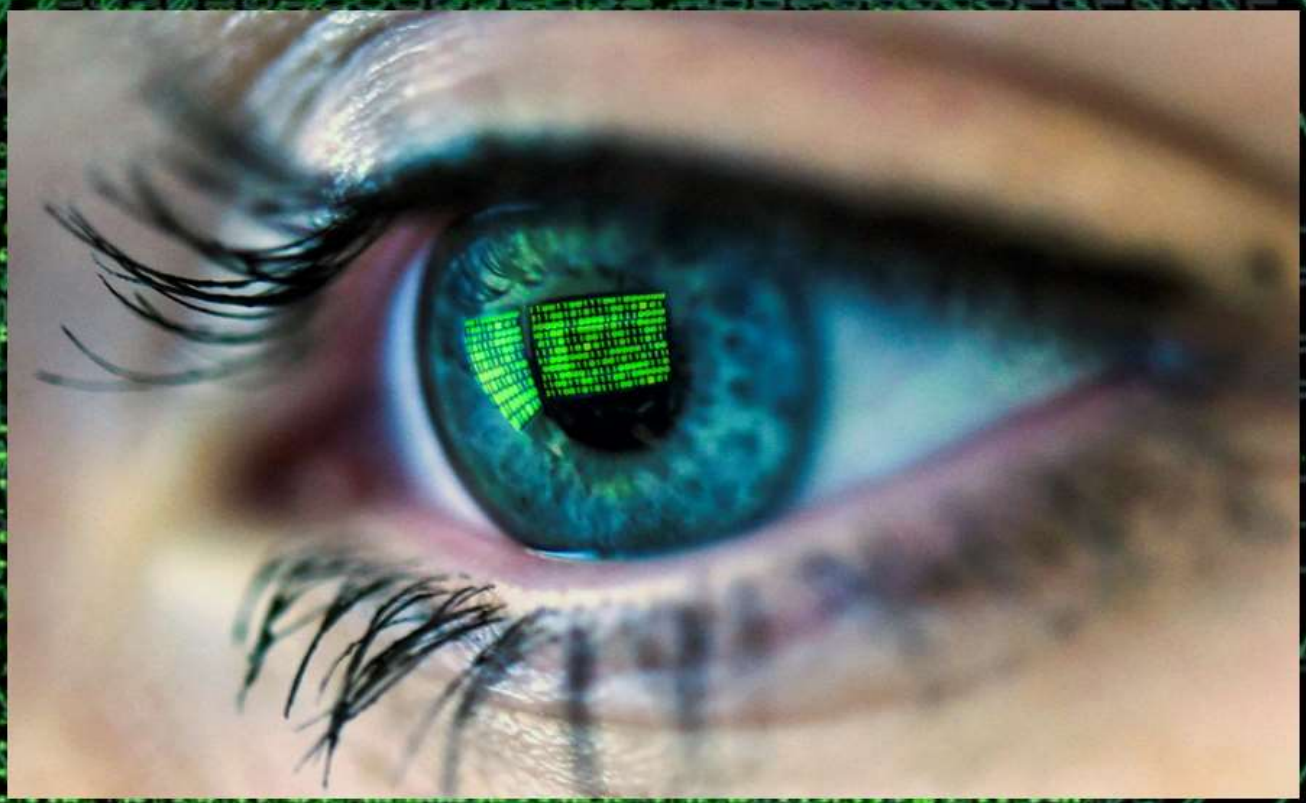
The Information Environment:



Competition & Conflict

A Mad Scientist Laboratory Anthology

This page intentionally left blank

Table of Contents

This page intentionally left blank

Introduction

The Information Environment (IE) is a unique space that demands our understanding, as the Internet of Things (IoT) and hyper-connectivity have democratized accessibility, extended global reach, and amplified the effects of its weaponization. Our strategic competitors and adversaries have been quick to grasp and employ it to challenge our traditional advantages and exploit our weaknesses.

- Russia and China confront us globally, converging IE capabilities with hybrid strategies to expand the battlefield across all domains and create hemispheric threats challenging us from home station installations (i.e., the Strategic Support Area) to the Close Area fight.
- Democratization of weaponized information empowers regional hegemons and non-state actors, enabling them to target the U.S. and our allies and achieve effects at a fraction of the cost of conventional weapons, without risking armed conflict.
- The Information Environment enables our adversaries to frame the conditions of future competition and/or escalation to armed conflict on their own terms.

The IE is the point of departure for all events across the Multi-Domain Operations spectrum. The Mad Scientist Initiative will explore information weaponization throughout our FY20 events with more to follow on the **Mad Scientist Laboratory**! This Anthology serves as a primer for our exploration, examining the convergence of technologies that facilitate information weaponization:

- **Artificial Influencers:** scraping social media accounts to build specialized 'bot armies' to precisely target populations across the full political spectrum using "knee-jerk" on-line affinities.
- **Deepfakes:** constructing videos that appear to make a person say or do something that they never said or did.
- **Artificial Intelligence (AI) Generative Adversarial Networks (GANs):** generating fully original faces, bodies, personas, and robust identities to conduct influence operations, seed doubt, and erode trust.
- **Direct Injects:** executing personalized psychological warfare attacks against civilian populations, Soldiers, and their families via immersive media (Augmented Reality/Virtual Reality/Mixed Reality [AR/VR/MR] and 360º Video/Gaming).
- **Disruption/Corruption of Critical IT/Sensor Nodes:** probing and targeting via cyber attacks to upset and undermine trust and confidence in financial institutions and critical government and public functions via Supervisory Control and Data Acquisition (SCADA), voting, banking, and governance mechanisms.
- **Data Manipulation of AI Systems**: exploiting and spoofing data-dependent AI systems via the proliferation of sensors and ubiquitous communications.

Sit back and enjoy reading this Anthology – then engage and share your ideas with the Mad Scientist Community of Action!

Return to the Table of Contents

This page intentionally left blank

Chapter 1. The Information Environment (IE)

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 26 (5 Feb 18)

26. The Future of the Cyber Domain

"The force that is postured, resilient, and able to converge its capabilities across all domains will win. We must be that force." — Gen. David Perkins, Commanding General, U.S. Army Training and Doctrine Command

The Army must be prepared to fight across multiple domains and contested areas, to deter potential adversaries and rapidly defeat enemies. **Multi-Domain Battle** and the associated capabilities will ensure that future Soldiers and Joint Teams can fight, win, and survive on tomorrow's battlefields. The future of the Cyber domain is one of the most difficult aspects of the **Future Operational Environment (OE).** It is the domain most impacted by **speed, scope, and convergence**. **The 2050 Cyber Army Conference**, co-sponsored by the Army Cyber Institute and the United States Military Academy, on 13-14 September 2016 at West Point, New York, tackled this domain, defining Cyber Future Attributes and Alternative Cyber Futures.

Cyber Future Attributes:

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

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

Volatility. The pervasiveness and leverage of cyberspace infrastructure will likely have a destabilizing impact on global – and local – stability. Digitization and social media, for example, will blend "weaponized data" and potentially micro-target anyone on the planet. The multiplicity of potential actors – and the expansion of

the means at their disposal – can only be problematic for a stable operational environment.

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

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

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

…between land and cyberspace operations.

…between all the legacy domains, as cyberspace constitutes the connective ether that readily transfers effects from one domain to another.

…between time and space as enhanced information and communication technologies decrease the time and expand the reach of cyber actions.

…between electromagnetic (EMS) and cyberspace action.

…between defensive and offensive cyberspace operations to ensure one function informs the other.

…between information management (IM) and knowledge management (KM) as large data is leveraged to achieve advantage.

…between Army operational and institutional activities, creating an unprecedented level of interaction where operations impact institutional activities and vice-versa.

Alternative Cyber Futures:

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

The potential alternative cyber futures are as follows:

1. "Status Quo."

• **Description:** Cyberspace conflict tomorrow looks like that of today: there are high levels of crime and espionage, but no massive interstate cyber warfare

• **Relationship of Offense and Defense:** Favors Offense over Defense

• **Intensity and Kind of Conflict:** Conflict is as it is today: bad, but not catastrophic, with crime and spying

• **Intensity and Kind of Cooperation:** There is a healthy but limited sharing on response, standards, and cyber crime

• **Stability:** Relatively Stable

• **Likelihood:** Moderate

• **Why this is Possible:** Current trend line and massive attacks have not occurred yet, despite fifteen years of expectations

2. "Conflict Domain."

• **Description:** Cyberspace reflects a wide range of human conflict, just like air, land, space and maritime domains

• **Relationship of Offense and Defense:** Favors Offense over Defense

• **Intensity and Kind of Conflict:** There is a full range of conflict (i.e., crime, spying, embargos, and full-blown international conflict)

• **Intensity and Kind of Cooperation:** To be stable, cyber cooperation requires norms and regimes, just as in other domains

• **Stability:** Somewhat Stable

• **Likelihood:** High

• **Why this is Possible:** Other domains have generally supported a range of human activity, from commerce to conflict

3. "Balkanization."

• **Description:** Cyberspace breaks down into national fiefdoms: there is no single internet, just a collection of closely guarded and poorly interconnected national internets

• **Relationship of Offense and Defense:** Unknown / Depends

• **Intensity and Kind of Conflict:** Nations are possibly blocking access to content, to and from each other, although there may be fewer outright attacks

• **Intensity and Kind of Cooperation:** Cyber cooperation requires international agreement in order to interconnect national Internets

• **Stability:** Unknown / Depends

• **Likelihood:** Low

• **Why this is Possible:** Countries continue to build border firewalls, which UN control of the Internet could exacerbate

4. "Paradise."

• **Description:** Social and technological innovations make cyberspace an overwhelmingly secure place; where espionage, warfare, and crime are extremely difficult

• **Relationship of Offense and Defense:** Favors Defense much more than Offense

• **Intensity and Kind of Conflict:** All conflict is greatly reduced, although nations and other advanced actors retain some capability

• **Intensity and Kind of Cooperation:** Cooperation is critical if stability depends on norms, or unneeded if it depends on new technology

• **Stability:** Long-Term Stable

• **Likelihood:** Low

• **Why this is Possible:** New technologies or cooperation, long promised, could make security much easier

5. "Cybergeddon."

• **Description:** Cyberspace, always un-ruled and unruly, has become a "failed state" in a near-permanent state of disruption, including high levels of hacker, criminal, and terrorist activity

• **Relationship of Offense and Defense:** Favors Offense much more than Defense

• **Intensity and Kind of Conflict:** Every kind of conflict is not just possible, but ongoing, all of the time

• **Intensity and Kind of Cooperation:** Cooperation is either useless, as attackers always have the edge, or impossible, like trying to govern a failed state

• **Stability:** Long-Term Unstable

• **Likelihood:** Low

• **Why this is Possible:** Offense continues to outpace defense, as any new defensive technology or cooperation is quickly overcome

The key discriminator that drives alternative cyber futures in this model is the technology contest outcome between offensive and defensive cyber operations.

Conclusion:

The assessment of cyber offense ascendancy at the 2050 Army Cyber Conference reinforces Jason Healy's estimate that the **"Conflict Domain"** outcome is currently most likely. Recent actions by authoritarian regimes to attempt to control internet access and other uses of cyberspace –- together with concerns that the cyber domain, as currently constructed and managed, is simply too vulnerable and dangerous –- argue for a **"Balkanization"** outcome. Only if the disruptive material solutions previously described substantially mitigate future cyber vulnerabilities will the **"Paradise"** outcome be feasible.

For more information on warfare in the cyber domain from the 2050 Cyber Army Conference, see:

The Community of Hackers, Makers, and Innovative Thinkers Panel

Matthew Weaver's presentation, entitled **Pervasive Capability – Our Only Hope**

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Posts 32 (26 Feb 18)

32. Virtual War – A Revolution in Human Affairs (Part I)

(**Editor's Note:** Originally published under the same title in ***Small Wars Journal***, Mad Scientist Laboratory is pleased to have **COL(R) Stefan J. Banach** distill his compelling article into several guest blog posts. The article is a crystal clear clarion call for the need to design a lasting national technology-based policy, strategy, and doctrine in the face of increasingly agile adversaries.)

War, of any kind, is the ultimate failure of mankind. Yet, in the course of human endeavors, we have found another way in which to wage global war – in this case, **Virtual War in Virtual Battle Space**. The **"Technology Singularity"** espoused by Vernor Vinge and **Ray Kurzweil**, is the fundamental source and accelerant for Virtual War. The Vinge and Kruzweil articulation of the "Singularity" of biological and machine intelligence **is much closer than most of us understand.** The majority of the people in the world are caught up in the inertia of everyday activities, and the emergence of Virtual War is opaque to most of us. To that end and for clarity, the world is experiencing **Virtual War – A Revolution in Human Affairs**.

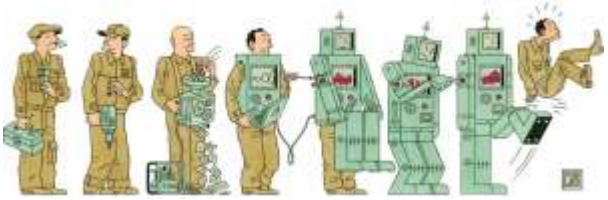
Virtual War transcends the "normal" revolutions in military affairs or traditional security rubrics that are discussed in Pentagon forums, within the defense industrial base, and among law enforcement agencies. Virtual War is **drastically transforming global human affairs** as we know them, and in ways that we do not yet understand. Eric Schmidt got it right when he opined that,

"the Internet is the first thing that humanity has built that humanity doesn't understand, it is the largest experiment in anarchy that we have ever had."

Virtual War is a **global systems approach** to achieve **social control**. Virtual War heuristics include: offensive and defensive **cyber capabilities**, social media, information operations (e.g., "Fake News"), **artificial intelligence**, stealth technologies, and cloaking techniques. The end game is to control and influence the will of a person, group, or larger population to achieve **ideological objectives** over time in support of a cause or a specific sponsor.

The United States, and indeed the world, is experiencing the birth pains of the coming **exponential technological change** that Vinge and Kurzweil predicted in the 1990's, and in 2005. Let the drastically reduced lifespans of **commercial companies** be a guide in this regard. The average age of an S&P 500 company is currently under 20 years, decreased from 60 years in the 1950s, according to Credit Suisse. The Wall Street firm says the trend is accelerating and blames the **disruption** on **unprecedented technological advancements**. In that vein, Andy Serwer, Editor-in-Chief of Yahoo Finance, asked this important question at the 2018 Davos World Economic Forum,

"*If robots, AI, nanotechnology, machine learning, and 3D printing are going to be doing all the work, what the heck will human beings do nine to five?*"



This question portends more challenges than simply the **re-training** and the **re-education** of a pending massive unemployed work force. The world has seen, since the events on 9/11, that large populations of **unemployed** or **under-employed** people are not helpful in terms of **maintaining global security and stability**.

Tangentially, sixteen years of **attrition warfare** and the banality associated with fighting predominantly in **Physical Battle Space** are **financially unsustainable**. The National Security Act of 1947, which is the basis of U.S. National Security, is **seventy-one years old** and is **collapsing** under the weight of Virtual War exigencies. As Peter Drucker noted,

"The greatest danger in times of turbulence is not the turbulence; it is to act with yesterday's logic."

The **new normal**, inherent in Virtual War, is the unprecedented **kinetic maneuvering** of one civilian population against another, which has produced hundreds of **mass casualty events** around the world since 9/11. The civilian vs. civilian terror attacks on 9/11 were planned using the **Internet of Things (IoT)** – in Virtual Space – prior to the execution of the physical attacks on the respective civilian targets in the United States. Hundreds of other terror attacks have taken place around the world since 9/11, and were **planned and coordinated in Virtual Space before the horrific attacks took place in Physical Space.** What will the world's **security paradigm** for warfare and law enforcement look like when the IoT **evolves** to the **Internet of Everything (IoET)**, that includes much more powerful **Nano-Biologically enhanced human beings**?

Non-lethal Virtual Space activities also occur continuously around the world in social and political domains that target domestic and foreign matters, with the aim to gain and maintain control of a particular narrative to **influence** an audience **to act in a certain ideological manner**. The growing liminality which exists today, by way of virtual space activity, is causing a **truth crisis**, as the velocity of human interaction and the velocity of information is at an all-time high. The average person does not know what to believe given the **ubiquity of information** and the **obvious bias** in government and within traditional and non-traditional media sources.

On the socio-economic front, there is a **growing divide** between the rich and poor, as the middle class struggles with sustainability. There is also a **widening chasm** between globalist and nationalist. The 1648 Westphalian nation-state model is at odds with a growing number of **emergent empowered actors** who do not rely on monolithic state

entities to govern their behavior in virtual or physical space. Each of these aforementioned variables are all interdependently joined and, to varying degrees, are **technologically driven fissures** in the world today.

Per Kurzweil's prose, future changes will be tantamount to a technological tsunami – which is now at our doorstep, in the context of the evolutionary timeline. Given the accelerating pace of technological advancements, we should **expect significant social change**. An unprecedented rupture of all the classic learning, leadership, management, strategy development, planning, and governance archetypes that are in existence today is absolutely possible. This externality will **move the world from** its current state of **complexity to chaos**. The end result will be the first of many instances where biological and machine intelligence **forever transforms warfare and our existence as we know it**.

The pending exponential technological advancements will move civilization to a completely new era. This will be an era where humans will not be able to survive without machine intelligence, augmented synthetic strength, and artificial stealth capabilities on the web or in physical space. Subterranean and extra-terrestrial options will be sought to support life and will be made possible by new technological advancements that were previously unimaginable. **The nation-state or actors who can learn the fastest, and optimally frame and reframe their strategies the best, will rule the day in a world that fights predominantly in Virtual Space, and only as necessary in Physical Space, as it is too costly on multiple fronts.**

[Return to the Table of Contents]

Mad Scientist Laboratory Blog Posts 37 (19 Mar 18)

37. Virtual War – A Revolution in Human Affairs (Part II)

(**Editor's Note:** Originally published under the same title in **Small Wars Journal**, Mad Scientist Laboratory is pleased to present Part II of our guest post by **COL(R) Stefan J. Banach,** distilling the essence of his original article. Part I may be read **here**.)

Framing and naming the **Virtual War paradigm** is a challenge for leaders today. The United States' leaders, who have responsibility to win the Nation's wars, have **lost personal mastery for warfare** in our time. The U.S. is fighting the wrong war, with the wrong policies, strategies, doctrine, tactics, techniques, and procedures. The **logic for warfare in our time is askew**, as we have seen at previous junctures in history. The value of mechanization versus the horse and the application of air power on modern battlefields during the 1919-1939 inter-war period are notable historical examples where **new technological advantages were not immediately appreciated by "the experts."**

Asymmetric Warfare, Political Warfare, Gray Zone Operations, Hybrid Warfare, Cyber Warfare, Cognitive Maneuver, et al., are competing heuristics that are bantered about continuously in security think tanks and in the halls of the Pentagon in an attempt to frame and name the **paradigm for warfare in this era**. Each of the aforementioned warfare nomenclatures and frameworks that are being used to describe warfare today are propagated in the **Virtual**

Domain and are further shaped in the **Cognitive** and **Moral Domains**, before they are manifested in the **Physical Domain** environments, which include: air, land, sea, and space.

The entity that controls the Virtual Domain and masters Virtual War Campaigning first, will indirectly achieve social control, and will win every war they engage in, at pennies on the dollar.

The Russian Gerasimov Doctrine and the **Chinese 2025 Strategic Plan** are both indirect approaches to **achieving social control** of domestic and foreign populations through the use of **Virtual War technology driven conventions.**

Social Control is the goal of Virtual War. China and Russia are well suited in this pursuit given their respective **repressive governance cultures.**

Invoking Sun Tzu is appropriate, as he summed up the goal of Social Control in this quote,

"The supreme art of war is to subdue the enemy without fighting."

Global "Social Control" is possible for the first time in the history of the world. **Burgeoning Social Control capabilities** are nested in: global satellite imagery, swarms of civilian and military aerial drones, public camera surveillance systems in our "smarter cities," iPhone tracking protocols, Fitbit devices, the internet, artificial intelligence, DNA, Social Security numbers, Driver's License numbers, Credit

Reports, online personal health records, and all the associated digital, personal, and financial contrivances which exist today.

In the years ahead, the Social Control challenge will become acute as **every human being will potentially have bio-medical nanotechnologies embedded in them to ensure optimal health.** Each of these medical Nano devices will have a **digital interface** that presents both new opportunities for **increased wellness** and **new vulnerabilities.** Humans will be susceptible to the traditional biological viruses which exist today. New technologies will need to be developed to protect us from artificial virus "infections" that could be **mass transmitted** in **targeted societies**, using the embedded Nano medical implants that will serve as the host within our bodies.

Metaphorically, the overwhelming propensity for **Physical Battle Space Maneuver** is the **United States' modern-day Maginot Line.** Like the French from 1919-1939, the U.S. has spent more money than all of its Allies combined in the Global War on Terrorism (GWOT) since 2001, executing Physical Battle Space Maneuver activities.

Like the French prior to WWII, the United States' leadership is **preparing for the last war it won** and does not see the **Virtual Blitzkrieg** that is upon it every day. There is an **ongoing complete envelopment of all the significant U.S. national interests** by way of Virtual War – or – Virtual Battle Space Maneuver, and it is happening right in front of us.

Creating an effective **Virtual War acumen** requires a **systemic reframe of leadership development** and the **creation of non-standard doctrine, tactics, techniques and procedures** for how our national security forces and law enforcement agencies compete in Virtual Space.

Virtual Space is the decisive terrain and securing it is the decisive operation.

For additional information on Russian and Chinese initiatives to win the Virtual War, download and review Timothy L. Thomas' works addressing these topics at the **Foreign Military Studies Office (FMSO) Bookshelf.**

COL(R) Stefan J. Banach *concluded his military service as the U.S. Army's 11th Director of the School of Advanced Military Studies (SAMS). As the SAMS Director, he led the development of the initial Design Methodology concepts and doctrine for the U.S. Army from 2007-2010. He is a Distinguished Member of the 75th Ranger Regiment and served in that organization for nine years, culminating with command of the 3rd Ranger Battalion from 2001-2003.*

Return to the Table of Contents

Chapter 2. IE Trends

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 123 (25 Feb 19)

123. Decision in the 21st Century

[**Editor's Note:** Mad Scientist Laboratory welcomes returning guest blogger **Matthew Ader**, whose submission builds upon his previous post regarding the demise of strategic and operational deception and surprise. Given the ascendancy of finders, Mr. Ader argues for the use of profoundly decisive impacts, achieved through information operations and minimal kinetic force, to "generate maximum hysteria" and bend the will of our adversaries' populations in order to achieve our objectives.]

The future battlespace will be dominated by the **finders**, not the hiders. Finder capabilities are effective and are only growing more so, leveraging **cross-domain surveillance** through cheap satellites, **unmanned systems**, and open source intelligence. This is augmented by the ongoing proliferation of precision long-range fires. In this environment, large unit manoeuvres to achieve decision favoured by the Joint Force will not be possible. Instead, kinetic action should be used to catalyse fear and dissatisfaction among the enemy civilian population, leading to pressure for a negotiated end to conflict.

Why is decisive kinetic manoeuvre no longer possible?

Logistics. Specifically, the practicalities of supplying a force in a finder dominated environment. During Operation Desert Storm, the fuel consumption rate per day for the U.S. VII and XVIII ABN Corps was about 4.5 million gallons. Ammunition requirements were about 14,000 tons a day.[1] Logistics support at this scale can neither be foraged nor arranged ad-hoc. Modern warfare depends on a robust supply network to deliver the requisite food, fuel, ammunition, and spare parts, when and where they are needed, to sustain the fight. In the First Gulf War, that was achieved by a handful of well provisioned logistics bases close to the line of advance. In the Second Gulf War,

logistics ran on a just in time model, with supply dependent on "**frequent, reliable distribution rather than on large forward stockpiles**."

Both of these models are no longer viable in the future operating environment. Large logistics bases will be highly vulnerable to cruise, ballistic, and conventional artillery fire. Drone attacks will also pose a significant challenge, aptly **demonstrated** in Kalynivka, Ukraine in 2017, where a single Russian quadcopter ignited a Ukrainian depot, destroying over 83,000 tons of ammunition. Challenges to air supremacy complicate the just in time delivery model. In a situation where units have only a few days of organic fuel and ammunition, a handful of missed convoys due to enemy air interdiction would prove disastrous. The unmanned threat is also present here. Autonomous 'mobile mines' could be deployed by air or artillery (à la Family of Scatterable Mines or FASCAM) onto lines of communication to complicate supply efforts.

This is not to say that logistics will be impossible. Promising innovations, particularly in using **autonomous vehicles**, could help with sustainment operations. Nevertheless, from a volume standpoint, the **division-sized forces** envisioned to achieve decision in a contested environment may not be viable.

What do we do instead?

War is about **compelling our opponent to fulfil our will**. Up to this point, the most efficient way to do this in a conventional war has been, bluntly, to kill people and blow things up until the enemy government surrenders. Due to the limitations on logistics imposed by the finder's world, this is no longer possible. We need to find a new way to compel our opponent to fulfil our will.

Luckily, modern information technology provides the Army with a new way. **51% of people** with social media access (**about 2.5 billion**) use it as a source for news. Both of these numbers are likely to grow as connectivity increases in the developing world. However, news on social media is often accompanied and preceded by a bow wave of hysteria, rumours, and conspiracy. This can have direct real-world impact – **#AllEyesOnISIS** caused much of the Iraqi force defending Mosul to flee before they saw the enemy. That was a profoundly decisive impact, achieved through minimal kinetic force.

The U.S. Army currently considers information operations to be an important adjunct to kinetic action. However, in a finder dominated environment, this should be flipped on its head. Small kinetic offensives (the smaller, the easier for likely highly degraded logistics networks to support) designed to generate maximum hysteria among the enemy

population should be the watchword. The result will be viral fear and significant internal pressure to accede to U.S. demands.

In the digital, connected age, all the world is a stage. The Army must learn to weaponize theatrics.

If you enjoyed this post, please also read the following:

– Mr. Ader's previous post **War Laid Bare**.

– Our review of Mad Scientist **P.W. Singer** and co-author **Emerson T. Brooking**'s book **LikeWar — The Weaponization of Social Media**.

– **COL Stefan J. Banach**'s complementary posts on Virtual War – A Revolution in Human Affairs (**Parts I** and **II**).

Mr. Matthew Ader *is a first-year undergraduate taking War Studies at King's College London.*

---

[1]Pagonis, LTG William G., with Cruikshank, Jeffrey L., **Moving Mountains: Lessons in Leadership and Logistics from the Gulf War**, Harvard Business Review Press, 1 August 1992.

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 126 (7 Mar 19)

126. Nowhere to Hide: Information Exploitation and Sanitization

[**Editor's Note:** In today's post, Mad Scientist Laboratory explores how humankind's recent exponential growth in interconnectivity will continue to affect warfare in the Future Operational Environment. Using several contemporary use cases, we identify a number of vulnerabilities that have already been exploited by our adversaries. The U.S. Army must learn how to sanitize its information signatures while simultaneously exploit those presented by our adversaries. As previously stated on this site by COL **Stefan J. Banach** (USA-Ret.), "*Virtual Space is the decisive terrain and securing it is the decisive operation."*]

The **timeless competition** of finders vs. hiders is a key characteristic of the Future Operational Environment (FOE). Through the **proliferation of sensors** creating the Internet of Battlefield Things (IoBT), ubiquitous global communication, and pervasive personal electronic devices, the finders will be ascendant on the battlefield. They have more advantages and access than ever before – with the ability to make impactful non-kinetic action – and the hiders are creating bigger, enduring, and more **conspicuous signatures**. In the FOE, our ability to wade through the petabytes of raw sensor and communications data input to generate a Common Operating Picture and arrive at actionable courses of action will be significantly challenged. Will we be able to sanitize Blue Forces' signatures to prevent our adversaries from detecting and exploiting similar information, while simultaneously seeing through Red Forces' deception measures to strike decisively?

A recent example highlighting the inherent and unpredictable vulnerabilities presented by these emerging technologies is the incident involving personal fitness devices that **track users via GPS**. Many military personnel have used these devices to track personal performance while conducting physical fitness training. The associated tracking information was transmitted back to fitness-tracking company **Strava**, where it was aggregated and then published as maps that were then made available to the public. Unfortunately, these maps contained articulate outlines of PT routes in and around military bases, the locations of which were not intended to be made public. This now publically available information inadvertently provided our adversaries with sensitive information that, in years past, would have required considerable time and other resources to acquire.

In response, the DoD issued a memorandum through Deputy Defense Secretary **Patrick Shanahan** effectively **banning** the use of geolocation capabilities in operational areas. While there was swift policy resolution in this case, albeit after-the-fact, there are a number of continuing and emergent threats presented by the information age that still need to be addressed.

In the previous example, the culprit was a smart watch or fitness tracking device that is a companion piece to the smart phone. Removing or prohibiting these devices is less detrimental to the overall morale, spirit, and will power of our Soldiers than removing their cell phones — their primary means of voice, data, and social media connectivity — oftentimes their sole link with their family back home. Adversaries have already employed tactics designed to exploit vulnerabilities arising from Soldier cellphone use. In the Ukraine, a popular **Russian tactic** is to send spoofed text messages to Ukrainian soldiers informing them that their support battalion has retreated, their bank account has been exhausted, or that they are simply surrounded and have been abandoned. Taking it one step further, they have even sent false messages to the families of soldiers informing them that their loved one was killed in action. This sets off a chain of events where the family member will immediately call or text the soldier, followed by another spoofed message to the original phone. With a high number of messages to enough targets, an **artillery strike** is called in on the area where an excess of cellphone usage has been detected.

Similarly, a NATO red team was able to easily infiltrate their own forces through information gathered on social media sites – amassing locations, dates, and other data – to influence their Soldiers' behavior. **Facebook and Instagram** allowed them to track

Soldiers, determine exact locations of exercises, and identify all members of a certain unit.

Hamas employed a **similar tactic** against Israeli Defense Force soldiers, using fake accounts to pose as attractive women in honey trap operations to access sensitive operational information.

Each of these examples illustrate recent, low-cost, and effective means of deception. Device exploitation, the over-sharing of sensitive data, and the challenge in determining information credibility will only increase as connected devices continue to both proliferate and transition from being portable and wearable to **embeddable and implantable**. The following questions must be addressed by the U.S. Army:

- How can we sanitize ourselves to mitigate these and other vulnerabilities from adversely affecting us operationally on future battlefields?

- How do we ensure that the information we are receiving and processing is legitimate and that we are not being spoofed?

- How are we preparing to exploit similar vulnerabilities in our adversaries?

- Is this even possible in a hyper-connected and complex battlefield or are we destined to be on the wrong side of some future **Operation Fortitude**, where effective military deception helped ensure the success GEN Eisenhower's Great Crusade to liberate Europe from the Nazis in World War II?

One final thought — geolocation information and high resolution remote sensing capabilities, which only a short decade and a half ago were limited to a handful of national intelligence services, have entered into a new, democratized era. As recently demonstrated in **three warzone use cases**, anyone (including non-spacefaring nations, non-state actors, and super-empowered individuals) can now access current and past

imagery to generate high resolution, three dimensional views for geolocation, analysis, and (unfortunately) exploitation. The convergence of this capability with the proliferation of personalized information signatures truly means that there is "**Nowhere to Run, Nowhere to Hide**." (Crank it up with **Martha and the Vandellas**!)

If you enjoyed this post, please also read the following blog posts addressing the weaponization of social media, the future of battlefield deception, and virtual warfare:

- Our review of proclaimed Mad Scientist **P.W. Singer** and co-author **Emerson T. Brooking**'s book **LikeWar — The Weaponization of Social Media**.
- **Matthew Ader**'s posts on **War Laid Bare** and **Decision in the 21st Century**.
- COL (USA-Ret.) **Stefan J. Banach**'s complementary posts on Virtual War – A Revolution in Human Affairs (**Parts I** and **II**).

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 158 (1 July 19)

158. In the Cognitive War – The Weapon is You!

[**Editor's Note:** Mad Scientist Laboratory is pleased to publish today's post by guest blogger **Dr. Zac Rogers**, addressing the on-going cognitive war (i.e., what **COL Steve Banach** describes in as **Virtual War —** see his blog posts **Parts I** & **II**]). In the race to achieve a cognitive edge, Dr. Rogers cautions the West about hidden assumptions that may prove to be cognitive vulnerabilities — Enjoy!]

A growing portion of the national security, intelligence, and defense (NSID) communities in the US, UK, Europe, Australia, and elsewhere are exploring the concept of cognitive war. The idea is basically that irregular and unconventional methods and means, which increasingly include non-kinetic and non-lethal delivery and effects leveraging digital connectivity, have shifted the center of gravity of political conflict from a violent clash of arms on the conventional battlefield to a narrative contest among the population. In the process, traditional concepts within the art and science of violent political conflict associated with boundaries, thresholds, levels, and phases are all deeply disrupted.

While many in the NSID community are willing to accept we are fighting a cognitive war, few are willing to recognize the extent to which it is being lost. Losing the cognitive war raises another fashionable topic emerging lately – strategic surprise. This is not the **fight we thought** we would get; it is not the fight we've invested in; nor is it the fight we wanted. But it is the **fight we've got**. The radical shifts in how society is organized and how warfare is conducted have exposed the NSID community to strategic surprise.

Losing without fighting

Cognitive warfare is not only an attack on ***what we think***. It is an attack on our way of thinking. Not only about the conduct of warfare but about whole-of-nation security and prosperity. And one of its unique properties is the extent to which we do it to ourselves. We **participate**. The adversary, in the age of hyper-connectivity, need only show up, inject, nudge, exploit, and disappear. The concept of 'below the threshold' conflict becomes meaningless when we prove ourselves capable of losing without fighting. The threshold of what?

The target of this type of warfare is obvious enough. It is the **fabric of trust** which underpins and enables the most basic functionality of open society. Trust that extends beyond heredity and beyond the purely transactional is the fabric that supports every aspect of the nation's **strategic strength**. Instead of investing in the true strengths of open society after the Cold War, we have left it to atrophy in the hubristic belief that the open way of life was universalizing.

Gamers will get gamed

Easy to overlook often goes hand-in-hand with difficult to measure. Scientists really hate talking about this, but part of the reason for that overlooking is the resurgence of **Positivism**. Without always understanding it, and often without stating it, the majority of research and development in defence science and technology inherits both its epistemology and its methodology from Positivism. And R&D into the cluster of technologies associated with AI proceeds under many of the assumptions of **Behaviourism**.

These are currents in the historical drift of European thought – not arrows to truth. They are 'ways of thinking'. The unresolved controversies in these **Occidental** thought trajectories are many. The discomfort, if not outright dismissal, of the assumptions they accommodate by the scientific community amount to cognitive vulnerabilities. The heavy reliance on these communities by the NSID community means people in the latter should, at a minimum, be aware of the assumptions which so often go unstated by people in the former.

When Occidentalism and Positivism combine in the race for the next false dawn in technological supremacy, blind spots are produced. Believers in an 'AI race' should be wary. We in the West see this as an S&T contest, while largely ignoring its socio-political implications. For the Chinese, AI is politics, politics, politics. Is there something about non-Occidental cultural orientations that makes AI applicable to human affairs in ways not amenable to us? It's an important strategic question. Positivism, by masking the salience of cultural orientation, is an exploitable weakness of our epistemic communities in need of addressing.

Proceed with caution

When 'behavioural scientists' get excited about manipulating people, either for benign or malign ends, what is the effect on the fabric of trust open society depends on? Military organizations now scrambling to incorporate 'the cognitive' into their operational concepts face a steep curve and many roadblocks. Friction is not always a bad thing. Hubristic behavioural interventions into complex anthropological systems involving AI should be approached with great caution. Hidden assumptions are cognitive vulnerabilities, and what appears to be a branch of S&T competition could turn out to be a strategic *cul de sac* we might want to back out of later.

It's one thing to know thy enemy. In the cognitive war, it's more important than ever to know thyself.

If you enjoyed this post, please also see:

– **An Appropriate Level of Trust…**

– **Man-Machine Rules**, by **Dr. Nir Buras**

– **The Death of Authenticity: New Era Information Warfare**

Dr. Zac Rogers *PhD is Research Lead at the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance at Flinders University of South Australia. Research interests combining national security, intelligence, and defence with social cybersecurity, digital anthropology, and democratic resilience.*

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 16 (2 Jan 18)

16. Emergent Threat Posed by Super-Empowered Individuals

"… in calling Moriarty a criminal you are uttering libel in the eyes of the law, and there lies the glory and the wonder of it! The greatest schemer of all time, the organizer of every devilry, the controlling brain of the underworld — a brain which might have made or marred the destiny of nations. That's the man!" Sir Arthur Conan Doyle's Sherlock Holmes, describing his arch nemesis, Professor James Moriarty, in **The Valley of Fear**, published in 1914.

In Professor Moriarty, Conan Doyle created the prototypical Super-Empowered Individual (SEI). Today's SEIs — far from being fictional characters crafted to entertain readers from a gentler era — are real world, non-state actors that have been empowered by the on-going digital revolution, and are able to target and adversely affect the lives of millions around the globe. Mad Scientists addressed the threat posed by SEIs at the **Visualizing Multi Domain Battle 2030-2050** Conference, Georgetown University, 25-26 July 2017.

Per NIH, 1-2% of humans exhibit psychopathic behaviors

Characteristics of SEIs include:

• Highly connected and able to reach far beyond their geographic location.

• Access to powerful, low-cost commercial technology.

• Often more difficult to trace or attribute responsibility to actions.

• Not beholden to nation-state policies, ethics, or international law.

• Varying motivations (political, ideological, economic, and monetary).

• Often unpredictable, may not operate or execute like a traditional rational actor.

SEI-driven attacks will become increasingly common due to the proliferation of disruptive technologies — smart phones as multi-spectral sensors and jammers; commercial UAVs as precision-guided munitions; and high-powered computers with malware / infoware "weapons" — available to them.

This has been evidenced by the rise in global malware attacks, hacking of vehicles that operate with computers, and information operation campaigns through social media that have influenced policy, disrupted everyday life, and increased global security costs and concerns.

Wired recently reported on several Distributed Denial of Service (DDoS) attacks, launched by SEIs. This **article** reports that three college students have plead guilty to creating and launching **Mirai**, *"… an unprecedented botnet—powered by unsecured internet-of-things devices like security cameras and wireless routers—that unleashed sweeping attacks on key internet services around the globe,"* slowing or stopping the internet for most of the eastern United States. Their motive – *"trying to gain an advantage in the computer game Minecraft."*

According to FBI Special Agent Elliott Peterson, ***"DDoS at a certain scale poses an existential threat to the internet…. Mirai was the first botnet I've seen that hit that existential level."***

Cyber capabilities such as this, coupled with the widespread proliferation of deadly technologies and associated tactics, techniques, and procedures, provide **SEIs with the capability to disrupt, degrade, and deny Army forces across multiple domains and the reach to interdict them at home station, as well as while deployed.**

These attacks, however, need not necessarily be broad DDoS operations; SEIs can leverage these disruptive technologies to craft and execute **personalized warfare** attacks against key leaders, Soldiers, and their families' via pressure points (e.g., social media, commerce, work, and financial transactions).

An individual armed with a high-powered computer and proficient coding, programming, and/or hacking capabilities could induce as much damage as an entire battalion of conventionally-armed belligerent forces.

These national and global security concerns are only worsened when future SEIs are able to obtain technologies and techniques that today are primarily limited to intelligence agencies. Meanwhile, states' ability to counter (or even deter) the malicious use of available technologies remains unclear.

SEI's ability to deliver effects previously limited to state actors raises the following questions regarding what constitutes an act of war:

• What are the boundaries associated with conflict between states and SEIs?

• How does the Army address surveilling, targeting, and engaging SEIs outside of current counterterrorism policy, regulations, and doctrine?

SEIs will impact the Future OE. The Army must address how it will address and counter this growing threat.

For further discussions on the ramifications of the digital age on geostability, see Dr. David Bray's presentation on **Blurred Lines and Super-Empowered Individuals: Is National Security Still Possible in 2040?** presented at Georgetown University.

Return to the Table of Contents

Chapter 3. IE Operations

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

LikeWar – The Weaponization of Social Media

The Death of Authenticity: New Era Information Warfare

***Damnatio Memoriae* through AI**

"I Know the Sound it Makes When it Lies" AI-Powered Tech to Improve Engagement in the Human Domain

Weaponized Information: One Possible Vignette

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

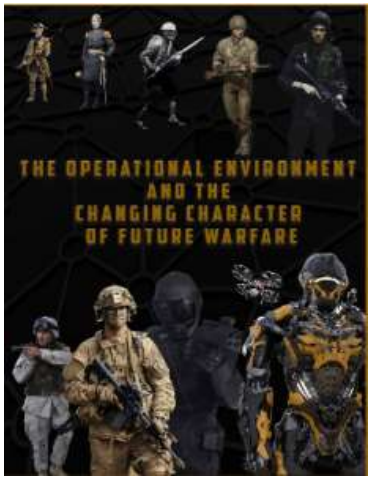
This page intentionally left blank

Mad Scientist Laboratory Blog Post 87 (01 Oct 18)

87. LikeWar — The Weaponization of Social Media

[**Editor's Note:** Regular readers will note that one of our enduring themes is the Internet's emergence as a central disruptive innovation. With the publication of proclaimed Mad Scientist **P.W. Singer** and co-author **Emerson T. Brooking**'s ***LikeWar – The Weaponization of Social Media***, Mad Scientist Laboratory addresses what is arguably the most powerful manifestation of the internet — Social Media — and how it is inextricably linked to the future of warfare. Messrs. Singer and Brooking's new book is essential reading if today's Leaders (both in and out of uniform) are to understand, defend against, and ultimately wield the non-kinetic, yet violently manipulative effects of Social Media.]

> *"The modern internet is not just a network, but an ecosystem of 4 billion souls…. Those who can manipulate this swirling tide, steer its direction and flow, can…. accomplish astonishing evil. They can foment violence, stoke hate, sow falsehoods, incite wars, and even erode the pillars of democracy itself."*



As noted in ***The Operational Environment and the Changing Character of Future Warfare***, Social Media and the Internet of Things have spawned a revolution that has connected "*all aspects of human engagement where cognition, ideas, and perceptions, are almost instantaneously available*." While this connectivity has been a powerfully beneficial global change agent, it has also amplified human foibles and biases. Authors Singer and Brookings note that humans by nature are social creatures that tend to gravitate into like-minded groups. We "Like" and share things online that resonate with our own beliefs. We also tend to believe what resonates with us and our community of friends.

> "*Whether the cause is dangerous (support for a terrorist group), mundane (support for a political party), or inane (belief that the earth is flat), social media guarantees that you can find others who share your views and even be steered to them by the platforms' own algorithms… As groups of like-minded people clump together, they grow to resemble fanatical tribes, trapped in echo chambers of their own design*."

Weaponization of Information

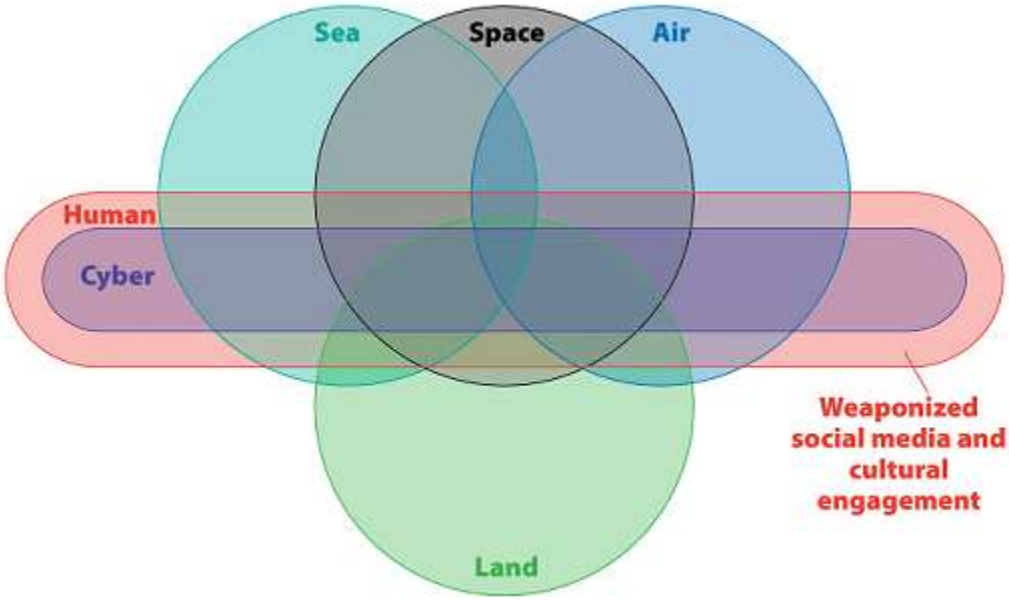
The advent of Social Media less than 20 years ago has changed how we wage war.

> "*Attacking an adversary's most important center of gravity — the spirit of its people — no longer requires massive bombing runs or reams of propaganda. All it takes is a smartphone and a few idle seconds. And anyone can do it*."

Nation states and non-state actors alike are leveraging social media to manipulate like-minded populations' cognitive biases to influence the dynamics of conflict. This continuous on-line fight for your mind represents "*not a single information war but thousands and potentially millions of them*."

LikeWar provides a host of examples describing how contemporary belligerents are weaponizing Social Media to augment their operations in the physical domain. Regarding the battle to defeat ISIS and re-take Mosul, authors Singer and Brookings note that:

> "*Social media had changed not just the message, but the dynamics of conflict. How information was being accessed, manipulated, and spread had taken on new power. Who was involved in the fight, where they were located, and even how they achieved victory had been twisted and transformed. Indeed, if what was online could swing the course of a battle — or eliminate the need for battle entirely — what, exactly, could be considered 'war' at all?*"



Even American gang members are entering the fray as **super-empowered individuals**, leveraging social media to instigate killings via "*Facebook drilling*" in Chicago or "*wallbanging*" in Los Angeles.

And it is only "*a handful of Silicon Valley engineers*," with their brother and sister technocrats in **Beijing**, St. Petersburg, and a few other global hubs of Twenty-first Century innovation that are forging and then unleashing the code that is democratizing this virtual warfare.

Artificial Intelligence (AI)-Enabled Information Operations

Seeing is believing, right? Not anymore! Previously clumsy efforts to photo-shop images and fabricate grainy videos and poorly executed CGI have given way to sophisticated **Deepfakes**, using AI algorithms to create nearly undetectable fake images, videos, and audio tracks that then go viral on-line to dupe, deceive, and manipulate. This year, **FakeApp** was launched as free software, enabling anyone with an artificial neural network and a graphics processor to create and share bogus videos via Social Media. Each Deepfake video that:

> *"… you watch, like, or share represents a tiny ripple on the information battlefield, privileging one side at the expense of others. Your online attention and actions are thus both targets and ammunition in an unending series of skirmishes*."

Just as AI is facilitating these distortions in reality, the race is on to harness AI to detect and delete these fakes and prevent "***the end of truth***."

If you enjoyed this post:

– Listen to the accompanying **playlist** composed by **P.W. Singer** while reading ***LikeWar***.

– Watch **P.W. Singer's** presentation on **Meta Trends – Technology, and a New Kind of Race** from Day 2 of the **Mad Scientist Strategic Security Environment in 2025 and Beyond Conference** at Georgetown University, 9 August 2016.

– Read more about virtual warfare in the following Mad Scientist Laboratory blog posts:

— MAJ Chris Telley's **Influence at Machine Speed: The Coming of AI-Powered Propaganda**

— COL(R) Stefan J. Banach's **Virtual War – A Revolution in Human Affairs** (**Parts I** and **II**)

— Mad Scientist Intiative's **Personalized Warfare**

— Ms. Marie Murphy's **Virtual Nations: An Emerging Supranational Cyber Trend**

— Lt Col Jennifer Snow's **Alternet: What Happens When the Internet is No Longer Trusted?**

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 149 (30 May 19)

149. The Death of Authenticity: New Era Information Warfare

[**Editor's Note:** Mad Scientist Laboratory is pleased to publish today's post, heralding the advent of the post-truth era with the convergence of deepfakes, AI-generated bodies and faces, and AI writing technologies. These tools are revolutionizing the nature of competition and could have a devastating impact on nations' will to fight once competition has transitioned into armed conflict — Beware! (Note: Some of the embedded links in this post are best accessed using non-DoD networks.)]

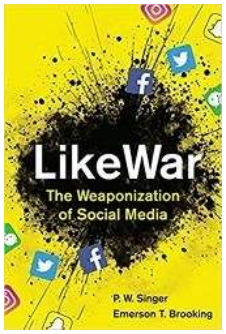
> "*Three things cannot be long hidden: the sun, the moon, and the truth*"
> – **Siddhārtha Gautama**, the Buddha

Even this quote is **not entirely truthful**. What the Buddha really said was, "*Monks, there are these three things which shine forth for all to see, which are not hidden. Which three? The disc of the moon shines for all to see; it is not hidden. The disc of the sun does likewise. The Dhamma-Discipline* [dhamma-vinaya] *of a Tathagata* [Buddha] *shines for all to see; it is not hidden. These are the three things*."

But what if the truth becomes increasingly hard to discern? What if authenticity (i.e., full trustworthiness) is actually dying? The advent of the Internet brought with it the global spread of a myriad of hoaxes, urban myths, and the dreaded fake news. During the first decade in the twenty-first century, it was a recurrent weekly theme to see a fake celebrity death spread like wildfire.

While propaganda, deception, and information warfare has existed in some form or fashion from ancient times through modern history (e.g., Soviet ***maskirovka***), the convergence of technology and these political/warfare areas has truly weaponized disinformation on social media and throughout the political arena. This employment of new era information warfare seeks not to necessarily change opinions, but erode trust in conventional institutions, induce trepidation and doubt, and instill a sense of indecisiveness that allows adversaries and nefarious actors the chance to achieve their ends, *fait accompli.*

The emergence of weaponized social media, as typified in **P.W. Singer**'s "**LikeWar — The Weaponization of Social Media,**" is potentially just the tip of the iceberg compared to the emergence of some disruptive technologies in the artificial intelligence (AI) and machine learning (ML) sector. There are three specific AI/ML applications that could bring about the Death of Authenticity:



1) Deepfakes – Videos that are constructed to make a person appear to say or do something that they never said or did (similar to the appearances of Presidents John F. Kennedy, Lyndon B. Johnson, and Richard M. Nixon with Forrest Gump in the 1996 eponymous movie). AI has improved this capability so greatly that it is extremely difficult to discern deepfakes from real video by the naked eye and ear – as seen in recent examples such as acclaimed director Jordan Peele's **video of President Obama**. Deepfakes are alarming to national security experts as they could trigger accidental escalation, undermine trust in authorities, and cause unforeseen havoc. **Significant efforts** are underway to use the same technologies enabling deep fakes – AI/ML – to detect and counter them.

2) AI-Generated Bodies and Faces – AI-driven Generative Adversarial Networks (GANs) are being used to generate entirely original and fake **faces** and even whole **bodies**. While this technology has commercial applications in such areas as video game design, online clothing sales, and human resources, it also has a profound impact on information warfare. Troll and bot armies are of increasing concern to military and government officials who worry about their effects on political environments and electoral outcomes. Imagine if you will this same threat to the political and governmental landscape with amplified psychological effects from realistic bodies and faces that humanize such bots.

3) AI Writing – A **text generation tool** created by OpenAI, a research institute based in San Francisco, can now compose original text in realistic prose. The tool is continuing to improve, generating convincing headlines, posts, articles, and comments, entirely free from human input. AI's ability to generate new, fictional material is not in and of itself a significant concern – humans can and do this now (see **The Onion** and other satirical sites). What is worrying is the scale at which this can be accomplished. What if AI were to generate hundreds of thousands, if not millions of comments or posts, geared at either supporting or undermining a specific issue or cause?

The convergence of these three technologies could spell the death of authenticity. How will the masses struggle with being flooded with a steady stream of AI-generated deepfakes constantly conveying mixed messages and troll armies that are indistinguishable from their fellow citizens, students, and Soldiers? A constant bombardment of messages by false media and fabricated personalities has the potential to erode the relationship between governments and their citizens, provoking severe reactions throughout the world and leading people to question the very reality they believe.

If you enjoyed this post, please read:

– **MAJ Chris Telley**'s post on the strategic threat presented by AI-enabled Information Operations in **Influence at Machine Speed: The Coming of AI-Powered Propaganda**.

– Our review of the **Australian Broadcasting Corporation**'s two part series on deepfakes and the **Deep Video Portraits** video from SIGGRAPH 2018 in the October 2018 edition of "**The Queue**" (see the first entry).

– Our review of Mad Scientist **P.W. Singer** and co-author **Emerson T. Brooking**'s book **LikeWar — The Weaponization of Social Media**.

– **COL Stefan J. Banach**'s complementary posts on Virtual War – A Revolution in Human Affairs (**Parts I** and **II**).

… and crank up **The Eurythmics**' ***Would I Lie to You?***

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 165 (29 July 19)

165. *Damnatio Memoriae* through AI

[**Editor's Note**: In today's post, proclaimed Mad Scientist and returning guest blogger **Ms. Marie Murphy** addresses the implications of weaponized Artificial Intelligence (AI) when employed in information operations. Truth and trust are the first causalities of this perception-altering capability!]

Artificial Intelligence (AI) is a tool that effectively enables machine-speed actions, posing new threats never before seen over the course of history. This disruptive capability can both erase existing data and create entirely false realities. If nefarious actors are able to effectively harness AI, the Army may potentially operate in a manufactured information environment with altered data guiding its decision-making. Using AI in this way is a competition-phase tactic that affects the will of people and deteriorates their trust, both within and about the Army.

Historical Precedence

The concept of altering or removing information from public memory has been around since the time of Ancient Rome. *Damnatio memoriae* is the contemporary term for the condemning of the memory of an emperor by the Senate posthumously.[1] The idea is "to erase a person as if he (or she) never existed."[2] The practice died out with the emerging prominence of the Catholic Church but resurfaced in Northern Italy during the Renaissance.[3] A "damnation of memory" was ordered when a new government took power in Florence, purging the powerful citizens and families of the old regime from societal recollection.[4] In the 20th century, at the height of the Soviet Union, **Josef Stalin** worked to remove any mention or figure of his political enemies from public view, to the point where they were edited out of textbooks and pictures.[5]

Today, history is repeating itself. China is attempting to remove all reference to the events that occurred in Tiananmen Square on 3-4 June 1989, and they have an advantage those in the past did not: AI. The absence of any public information about the events surrounding Tiananmen Square in contemporary China stems from the Chinese government's efforts to censor any mention or insinuation of the incident online and in reality. AI works at machine-speed to filter internet search results and social media posts to assist human censors.[6] A recent study proved the effectiveness of this campaign, showing that a meager 15% of Beijing University students could accurately identify the "tank man" photograph, one of the internationally recognized symbols of the protest.[7] While most people appear to be aware of the incident by the time they're well into their 20s, there is a general apathy toward, or even sympathy with the government amongst the current generation regarding the 1989 protests.[8]

Future Threat

AI can be weaponized in information and cyber warfare, which characterize the interactions between strategic competitors in the competition phase. However, it's often discussed in the context of lethal autonomy, man-machine teaming, or practical battlefield applications. But what happens when AI begins to psychologically alter the operational environment by changing the perceptions of both military and civilian personnel alike? Through the deletion or alteration of the past or the creation of a fabricated present, AI is a tool which aids in and speeds up the process of identifying, changing, and generating information. False narratives based on AI-manipulated or -generated information and media can originate from anyone, anywhere; developing and spreading rapidly with a detrimental effect on trust. This deterioration of trust moves in two directions: The Soldier not trusting the information they are given which is crucial for decision-making and combat performance, and civilians and other militaries not trusting the actions of the U.S. Army because their perceptions have been affected by AI-influenced content.

If AI, employed by a nefarious actor, is able to manipulate the information available about the past and deliver false information about the present, there is likely to be a strong impact on Soldier and Commander trust of any information received. Altering history to the point that it is impossible to discern what the truth is, and potentially basing decisions on inaccurate information about the past, could have unintended and devastating consequences. AI manipulations can also affect trust because of their applicability in enabling small-scale,

personalized warfare. A particular Soldier could be targeted with a computer-generated fake message from home that someone is very ill. This false information could cause a breakdown of trust and a rise in skepticism in the individual Soldier to the point that they begin to question every piece of information they're given, wasting valuable time and energy.

The Army is also facing the challenge of AI manipulating the perceptions of military and civilian personnel support elements. AI and those who program it can accomplish this by doctoring or deleting the records or social perceptions of prior Army actions. To create a false reality that corrupts the information environment, AI could be used to spread malicious rumors influencing international will and public opinion. One such rumor might be a manufactured atrocity. It would be incredibly hard to deny the alleged incident if there are audio and video recordings depicting it (even though that evidence is fabricated with the help of AI); the programmer could even use AI to create computer-generated people "on camera" giving false eye-witness accounts. If the public and other militaries whom the U.S. aligns with do not trust the Army, then operations will become strategically and tactically more challenging.

While AI may present the Army with many strategic and tactical benefits by providing machine-speed analysis and decision-making, it can also work counter to the Army's goals and initiatives. With other entities such as China developing AI at a rapid pace and willing to deploy it against its own citizens, the time of AI-enabled *damnatio memoriae* has arrived. Whether it be altering the past or creating a false present, AI-generated information may greatly impact future operability and trust of warfighters.

If you enjoyed this post, please also see:

Influence at Machine Speed: The Coming of AI-Powered Propaganda by **MAJ Chris Telley**

The Death of Authenticity: A New Era of Information Warfare

China's Drive for Innovation Dominance

*Proclaimed Mad Scientist **Marie Murphy** is a rising senior at The College of William and Mary in Virginia, studying International Relations and Arabic. She is a regular contributor to the Mad Scientist Laboratory, interned at Headquarters, U.S. Army Training and Doctrine Command (TRADOC) with the Mad Scientist Initiative last summer, and has returned as a consultant this summer. She was a Research Fellow for William and Mary's Project on International Peace and Security.*

Disclaimer: The views expressed in this article do not imply endorsement by the U.S. Army Training and Doctrine Command, the Army Futures Command, the U.S. Army, the Department of Defense, or the U.S. Government. This piece is meant to be thought-provoking and does not reflect the current position of the U.S. Army.

[1] "Damnatio Memoriae." *Livius.org*, updated June 23, 2019. https://www.livius.org/articles/concept/damnatio-memoriae/

[2] Petersen, Lauren Hackworth. "The Presence of 'Damnatio Memoriae in Roman Art." *Notes in the History of Art*, vol. 30, no. 2, 2011, p.1. *JSTOR.* www.jstor.org/stable/23208566

[3] "Damnatio Memoriae." *Livius.org*, updated June 23, 2019. https://www.livius.org/articles/concept/damnatio-memoriae/

[4] Petersen, Lauren Hackworth. "The Presence of 'Damnatio Memoriae in Roman Art." *Notes in the History of Art*, vol. 30, no. 2, 2011, p.1. *JSTOR.* www.jstor.org/stable/23208566

[5] Bond, Sarah. "How Do You Purge The Memory Of An Emperor." *Forbes.com*, April 11, 2017. https://www.forbes.com/sites/drsarahbond/2017/04/11/how-do-you-damn-the-memory-of-a-roman-emperor/#49228baf49b2

[6] Gilbert, David. "How China Is Wiping Memories of Tiananmen Square Off The Internet." *Vice News*, June 4, 2019. https://news.vice.com/en_us/article/7xge3b/chinese-dissidents-are-running-out-of-ways-to-remember-tiananmen-square

[7] Keng Kuek Ser, Kuang. "How China has censored words relating to the Tiananmen Square anniversary." *Pri.org*, Hune 4, 2016. https://www.pri.org/stories/2016-06-03/how-china-has-censored-words-relating-tiananmen-square-anniversary

[8] Fish, Eric. "Tiananmen Shaped China's History. But Chinese Millennials Have Mixed Views About Its Legacy." *Time*, June 3, 2019. https://time.com/5599060/china-millennials-tiananmen-anniversary/

Return to the Table of Contents

Mad Scientist Laboratory Blog Post 175 (12 Sep 19)

175. "I Know the Sound it Makes When It Lies" AI-Powered Tech to Improve Engagement in the Human Domain

[**Editor's Note:** Mad Scientist Laboratory is pleased to publish today's post by guest bloggers **LTC Arnel P. David**, **LTC (Ret) Patrick James Christian, PhD**, and **Dr. Aleksandra Nesic**, who use storytelling to illustrate how the convergence of Artificial Intelligence (AI), cloud computing, big data, augmented and enhanced reality, and deception detection algorithms could complement decision-making in future specialized engagements. Enjoy this first in a series of three posts exploring how game changing tech will enhance operations in the Human Domain!]

It is 2028. Lt Col Archie Burton steps off the British A400-M Atlas plane onto the hard pan desert runway of Banku Airfield, Nigeria. This is his third visit to Nigeria, but this time he is the commander of the Engagement Operations Group – Bravo (EOG-B). This group of bespoke, specialized capabilities is the British Army's agile and highly-trained force for specialized engagement. It operates amongst the people and builds indigenous mass with host nation security forces. Members of this outfit operate in civilian clothes and speak multiple languages with academic degrees ranging from anthropology to computational science.

Archie donned his **Viz glasses** on the drive to a meeting with local leadership of the town of Banku. Speaking to his AI assistant, "Jarvis," Archie cycles through past engagement data to prep for the meeting and learn the latest about the local town and its leaders. Jarvis is connected to a cloud-computing environment, referred to as "HDM" for "Human Doman Matrix," where scientifically collected and curated population data is stored, maintained, and integrated with a host of applications to support operations in the human domain in both training and deployed settings.

Several private organizations that utilize integrated interdisciplinary social science have helped NATO, the U.K. MoD, and the U.S. DoD develop CGI-enabled virtual reality experiences to accelerate learning for operators who work in challenging conflict settings laden with complex psycho-social and emotional dynamics that drive the behaviour and interactions of the populations on the ground. Together with NGOs and civil society groups, they collected ethnographic data and combined it with phenomenological qualitative inquiry using psychology and sociology to curate anthropological stories that reflect specific cultural audiences.

EOG-Bravo's mission letter from Field Army Headquarters states that they must leverage the extensive and complex human network dynamic to aid in the recovery of 11 females kidnapped by the Islamic Revolutionary Brotherhood (IRB) terrorist group. Two of the females are British citizens, who were supporting a humanitarian mission with the 'Save the Kids' NGO prior to being abducted.

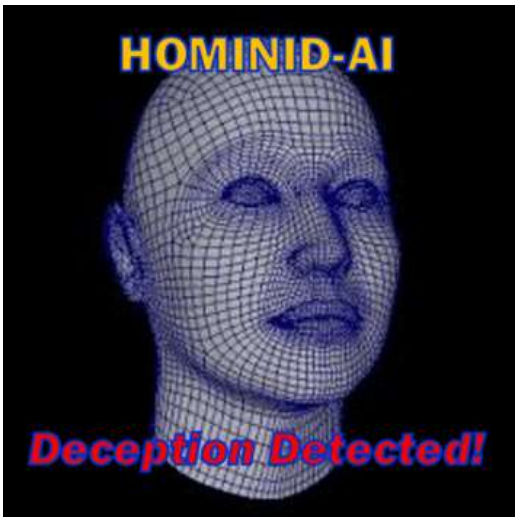
At the meeting in Banku, the mayor, police chief, and representative from Save the Kids were present. Archie was welcomed by handshakes and hugs by the police chief who was a former student at Sandhurst and knows Archie from past deployments. The discussion leaped immediately into the kidnapping situation.

> "*The girls were last seen transiting a jungle area North of Oyero. Our organization is in contact by email with one of the IRB facilitators. He is asking for £2 million and we are ready to make that payment*," said Simon Moore of Save the Kids.

Archie's Viz glasses scanned the facial expressions of those present and Jarvis cautioned him regarding the behaviour of the police chief whose micro facial expressions and eyes revealed a biological response of excitement at the mention of the £2M.

Archie asks "C*hief Adesola, what do you think? Should we facilitate payment?*"

> "*Hmmm, I'm not sure. We don't know what the IRB will do. We should definitely consider it though*," said Police Chief Adesola.



The Viz glasses continued to feed the facial expressions into HDM, where the recurrent AI neural network recognition algorithm, *HOMINID-AI*, detected a lie. The AI system and human analysts at the Land Information Manoeuvre Centre (LIMOC) back in the U.K. estimate with a high-level of confidence that Chief Adesola was lying.

At the LIMOC, a 24-hour operation under 77th Brigade, Sgt Richards, determines that the Police Chief is worthy of surveillance by EOG-Alpha, Archie's sister battlegroup. EOG-Alpha informs local teams in Lagos to deploy unmanned ground sensors and collection assets to monitor the police chief.

Small teams of 3-4 soldiers depart from Lagos in the middle of the night to link up with host nation counterparts. Together, the team of operators and Nigerian national-level security forces deploy sensors to monitor the police chief's movements and conversations around his office and home.

The next morning, Chief Adesola is picked up by a sensor meeting with an unknown associate. The sensor scanned this associate and the LIMOC processed an immediate hit — he was a leader of the IRB; number three in their chain of command. EOG-A's operational element is alerted and ordered to work with local security forces to detain this terrorist leader. Intelligence collected from him and the Chief will hopefully lead them to the missing females…

If you enjoyed this post, stay tuned for Part 2 on the Human Domain Matrix, Part 3 on Emotional Warfare in Yemen, and check out the following links to other works by today's blog post authors:

– Operationalizing the Science of the Human Domain by **Aleks Nesic** and **Arnel P. David**

– A Psycho-Emotional Human Security Analytical Framework by **Patrick J. Christian**, **Aleksandra Nesic**, **David Sniffen**, **Tasneem Aljehani**, **Khaled Al Sumairi**, **Narayan B. Khadka**, **Basimah Hallawy**, and **Binamin Konlan**

– Military Strategy in the 21st Century: People, Connectivity, and Competition by **Charles T. Cleveland**, **Benjamin Jensen**, **Susan Bryant**, and **Arnel P. David**

… and see the following MadSci Lab blog posts on how AI can augment our Leaders' decision-making on the battlefield:

– Takeaways Learned about the Future of the AI Battlefield

– The Guy Behind the Guy: AI as the Indispensable Marshal, by **Mr. Brady Moore** and **Mr. Chris Sauceda**

LTC Arnel P. David *is an Army Strategist serving in the United Kingdom as the U.S. Special Assistant for the Chief of the General Staff. He recently completed an Artificial Intelligence Program from the Saïd Business School at the University of Oxford.*

LTC (Ret) Patrick James Christian, PhD *is co-founder of* ***Valka-Mir*** *and a Psychoanalytical Anthropologist focused on the psychopathology of violent ethnic and cultural conflict. He a retired Special Forces officer serving as a social scientist for the Psychological Operations Task Forces in the Arabian Peninsula and Afghanistan, where he constructs psychological profiles of designated target audiences.*

Aleksandra Nesic, PhD *is co-founder of* ***Valka-Mir*** *and Visiting Faculty for the Countering Violent Extremism and Countering Terrorism Fellowship Program at the Joint Special Operations University (JSOU), USSOCOM. She is also Visiting Faculty, U.S. Army JFK Special Warfare Center and School, and a Co-Founder and Senior Researcher of Complex Communal Conflicts at Valka-Mir Human Security, LLC.*

Acknowledgements: *Special Thanks to the British Army Future Force Development Team for their help in creating the British characters depicted in this first story.*

Disclaimer: *The views expressed in this blog post do not necessarily reflect those of the Department of Defense, Department of the Army, Army Futures Command (AFC), or Training and Doctrine Command (TRADOC).*

Return to the Table of Contents

This page intentionally left blank

Mad Scientist Laboratory Blog Post 190 (7 Nov 19)

190. Weaponized Information: One Possible Vignette

[**Editor's Note:** The Information Environment (IE) is the point of departure for all events across the Multi-Domain Operations (MDO) spectrum. It's a unique space that demands our understanding, as the Internet of Things (IoT) and hyper-connectivity have democratized accessibility, extended global reach, and amplified the effects of weaponized information. Our strategic competitors and adversaries have been quick to grasp and employ it to challenge our traditional advantages and exploit our weaknesses.

- Our near-peers confront us globally, converging IE capabilities with hybrid strategies to expand the battlefield across all domains and create **hemispheric threats** challenging us from home station installations (i.e., the Strategic Support Area) to the Close Area fight.
- Democratization of weaponized information empowers regional hegemons and non-state actors, enabling them to target the U.S. and our allies and achieve effects at a fraction of the cost of conventional weapons, without risking armed conflict.
- The IE enables our adversaries to frame the conditions of future competition and/or escalation to armed conflict on their own terms.

Today's post imagines one such vignette, with Russia exploiting the IE to successfully out-compete us and accomplish their political objectives, without expending a single bullet!]

Ethnic Russian minorities' agitation against their respective governments in Estonia, Lithuania, and Latvia spike. Simultaneously, the Russian Government ratchets up tensions, with inflammatory statements of support for these ethnic Russian minorities in the Baltic States; coordinated movements and exercises by Russian ground, naval, and air forces adjacent to the region; and clandestine support to ethnic Russians in these States. The Russian Government started a covert campaign to shape people's views about the threats against the Russian diaspora. More than 200,000 twitter accounts send 3.6 million tweets trending **#protectRussianseverywhere**. This sprawling Russian disinformation

campaign is focused on building internal support for the Russian President and a possible military action. The U.S. and NATO respond…

The 2nd Cav Regt is placed on alert; as it prepares to roll out of garrison for Poland, several videos surface across social media, purportedly showing the sexual assault of several underage German nationals by U.S. personnel. These disturbingly graphic **deepfakes** appear to implicate key Leaders within the Regiment. German political and legal authorities call for an investigation and host nation protests erupt outside the gates of Rose Barracks, Vilseck, disrupting the unit's deployment.

Simultaneously, in units comprising the initial Force Package earmarked to deploy to Europe, key personnel (and their dependents) are targeted, distracting troops from their deployment preparations and disrupting unit cohesion:

- Social media accounts are hacked/hijacked, with false threats by dependents to execute mass/school shootings, accusations of sexual abuse, hate speech posts by Leaders about their minority troops, and revelations of adulterous affairs between unit spouses.
- Bank accounts are hacked: some are credited with excessive amounts of cash followed by faux "See Something, Say Something" hotline accusations being made about criminal and espionage activities; while others are zeroed out, disrupting families' abilities to pay bills.

Russia's GRU (Military Intelligence) employs AI Generative Adversarial Networks (GANs) to create fake persona injects that mimic select U.S. Active Army, ARNG, and USAR commanders making disparaging statements about their confidence in our allies' forces, the legitimacy of the mission, and their faith in our political leadership. Sowing these injects across unit social media accounts, Russian Information Warfare specialists seed doubt and erode trust in the chain of command amongst a percentage of susceptible Soldiers, creating further friction in deployment preparations.

As these units load at railheads or begin their road march towards their respective ports of embarkation, Supervisory Control and Data Acquisition (SCADA) attacks are launched on critical rail, road, port, and airfield infrastructures, snarling rail lines, switching yards, and crossings; creating bottlenecks at key traffic intersections; and spoofing navigation systems to cause sealift asset collisions and groundings at key maritime chokepoints. The fly-by-wire avionics are hacked on a departing C-17, causing a crash with the loss of all 134 Soldiers onboard. All C-17s are grounded, pending an investigation.

Salvos of personalized, "direct inject" psychological warfare attacks are launched against Soldiers via immersive media (Augmented, Virtual, and Mixed Reality; 360º Video/Gaming), targeting them while they await deployment and are in-transit to Theater. Similarly, attacks are vectored at spouses, parents, and dependents, with horrifying imagery of their loved ones' torn and maimed bodies on Artificial Intelligence-generated battlefields (based on scraped facial imagery from social media accounts).

Multi-Domain Operations has **improved Jointness, but exacerbated problems** with "*the communications requirements that constitute the nation's warfighting Achilles heel*." As units arrive in Theater, seams within and between these U.S. and NATO Intelligence, Surveillance, and Reconnaissance; Fires; Sustainment; and Command and Control inter-connected and federated tactical networks that facilitate partner-to-partner data exchanges are exploited with specifically targeted false injects, sowing doubt and distrust across the alliance for the Multi-Domain Common Operating Picture. Spoofing of these systems leads to accidental air defense engagements, resulting in Blue-on-Blue fratricide or the downing of a commercial airliner, with additional civilian deaths on the ground from spent ordnance, providing more opportunities for Russian Information Operations to spread acrimony within the alliance and create dissent in public opinion back home.

With the flow of U.S. forces into the Baltic Nations, real instances of ethnic Russians' livelihoods being disrupted (e.g., accidental destruction of livestock and crops, the choking off of main routes to market, and damage to essential services [water, electricity, sewerage]) by maneuver units on exercise are captured on video and enhanced digitally to exacerbate their cumulative effects. Proliferated across the net via bots, these instances further stoke anti-Baltic / anti-U.S. opinion amongst Russian-sympathetic and non-aligned populations alike.

Following years of scraping global social media accounts and building profiles across the full political spectrum, artificial influencers are unleashed on-line that effectively target each of these profiles within the U.S. and allied civilian populations. Ostensibly engaging populations via key “knee-jerk” on-line affinities (e.g., pro-gun, pro-choice, etc.), these artificial influencers, ever so subtly, begin to shift public opinion to embrace a sympathetic position on the rights of the Russian diaspora to greater autonomy in the Baltic States.

The release of deepfake videos showing Baltic security forces massacring ethnic Russians creates further division and causes some NATO partners to hesitate, question, and withhold their support, as required under Article 5. The alliance is rent asunder — Checkmate!

Many of the aforementioned capabilities described in this vignette are available now. Threats in the IE space will only increase in verisimilitude with augmented reality and multisensory content interaction. Envisioning what this Bot 2.0 Competition will look like is essential in building **whole-of-government countermeasures** and instilling resiliency in our population and military formations.

The Mad Scientist Initiative will continue to explore the significance of the IE to Competition and Conflict and information weaponization throughout our FY20 events — stay tuned to the MadSci Laboratory for more information. In anticipation of this, we have published **The Information Environment: Competition and Conflict Anthology**, a collection of previously published blog posts that serves as a primer on this topic and examines the convergence of technologies that facilitates information weaponization — Enjoy!

Return to the Table of Contents