

The only way to win World War III is to prevent it.
Dwight D. Eisenhower



Future Military Intelligence CONOPS and S&T Investment Roadmap 2035-2050 THE COGNITIVE WAR

Haugland, Edward L. SES, Senior Advisor for S&T Outreach and Technical ISR
February 20, 2019

Table of Contents

Bottom Line Up-Front (BLUF).....	1
Executive Summary	3
Key Findings, Challenges & Solutions	5
Proactive Influence and Predictive Analysis: Moving from Reactive to Proactive Posture	5
TECHNOLOGY IS NOT THE PROBLEM, IT'S DEFINING THE PROBLEM	9
WE ARE LOSING THE COGNITIVE WAR, WHILE FOCUSING NEAR SOLELY ON KINETIC.....	12
OUR BIGGEST HURDLES ARE CULTURAL (POLICY) AND STRUCTURAL (ORGANIZATION).....	19
CHALLENGES & SUGGESTED SOLUTIONS.....	21
<i>Addressing the Boring – But Truly Critical Stuff</i>	21
<i>A New Factory Floor – Overhauling and Retooling Our National Security Apparatus</i>	23
<i>Refining our Risk & Reward System</i>	25
<i>Remaking the Conscription System & Talent Management – Moving to Whole of Government (coalition/ nation as applicable)</i>	26
Future Operating Environment & the Character of Warfare 2035-2050.....	27
Future Military Intelligence CONOPS 2035-2050.....	28
Future Intelligence CONOPS - Threat & OPERATING Scenarios 2035-2050	33
<i>Bio-Warfare: Realizing Precise Elimination – 23&Xi</i>	33
<i>Lone-Wolf and Virtual Nation Chaos</i>	35
<i>Mega City & Virtual Elimination</i>	36
Future Intelligence S&T Investment Roadmap 2035-2050.....	39
Future S&T Investments 2035-2050: Examples for Consideration	41
Appendix A: Information as Joint Function, SECDEF memo, 9-15-2017	44
Appendix B: About the Author	45
Appendix C: About the Army Futures Command Community of Interest (AFC COI) & Basis and Background for Projections, Findings and Assessment	46
Appendix D: Concept 2015	49
Appendix E: Enterprise Architecture Depiction	51
Bibliography	53

Bottom Line Up-Front (BLUF)

There are four major findings about operations critical to the effectiveness and success of future of intelligence operations in 2035-2050 and beyond. The findings apply broadly not only to military intelligence, but the greater Intelligence Community (IC), the DoD, and by default to several other elements of our federal national security framework. However, realizing the Future Intelligence CONOPS 2035-2050 projection assumes addressing the findings. If not, it highly probable intelligence operations will continue to mimic the current reactive posture of today.

The four findings:

- **The IC and DoD, created in 1947, continue to function in a primarily reactive posture, using the industrial age processes of the era in which they were created.** Our IC and DoD were created during the industrial age, by the National Security Act of 1947. Their structure and functional roles were respectively to prepare for war and providing Indications and Warning (I&W). These functions are inherently reactive. Proactive influence requires significant forethought, well thought strategy, and sustaining strategic planning priorities. Strategy drives tactical efforts towards desired impact, influence and outcome. However, our tendency (perception and reality) is to chase the new “shiny objects” (e.g., AI/ML, Cyber, etc.), throw solutions at the wall, see what sticks and then repeat. We tend to operate as glorified reactive action officers, whereby we create crises, solve the immediate crises, pat ourselves on the back, then repeat – vice, looking and planning strategically and driving tactical efforts in line with strategy. The processes remain mostly unchanged and stick in the industrial age. In other words, we are waiting for the paradigm or environment to change, rather than taking a proactive approach and driving the change outcomes we desire. **To enable and provide future successful and effective intelligence operations, we must move from a predominately reactive to proactive posture.**
- **Information & democratization of technology has changed the character of warfare.** A 2017 memorandum (Appendix A: Information as a Joint Function, September 15, 2017) from the SECDEF created “Information” as the seventh joint function states “...Information is such a powerful tool that it is recognized as an instrument of national power. The advent of the internet, the expansion of information technology...have dramatically impacted operations and changed the character of modern warfare...the elevation of Information to a joint function impacts all operations and has implications across doctrine, organization.” Despite the plethora of new data and information sources, advances in information technology to utilize such information, we continue to react/respond to every new threat, new technology, new data, or new adversarial capability. Rather, we need to take a step back, think through and clearly define the problem, the type of functions or approaches that can be applied, identify and allocate the right type of expertise and resources, and then ensure we follow the motto “form to function.” Our current approach tends to view technology as part of the problem. **We must understand that technology is not the problem, it’s defining the problem.**
- **2018 National Security and Defense Security Strategies address the new character of warfare.** The 2018 NSS states “...Majority of adversary efforts in Competition phase (short of armed conflict) ... (are) challenging our ability to deter aggression.” It is in the cognitive realm we are losing the ideological war on multiple fronts, we are losing our intellectual property, our adversaries are outmaneuvering us, and we are failing to achieve overmatch because we focus solely on kinetic options. While the kinetic is important, if we lose the cognitive war, it is unlikely we will ever reach kinetic action. The dangers surpass any challenges we have faced in our history, as the NSS speaks to the new and startling reality of modern warfare stating, “It is now undeniable that the homeland is no longer a sanctuary.” **Our biggest challenge, is that we are in the midst of a cognitive war that will last a millennia or longer, and our focus remains near solely on kinetic.**
- **Immediate investments are required to enable the success and effectiveness of future intelligence operations in 2035-2050 and beyond.** The key areas of investment include Architecture & Infrastructure; Communication; Human Capital; Information Access & Cognition: Proactive Influence/Predicative Analytics; and Integration / Leverage with others. These investments are required to build a foundation that enables proactive influence and predictive analysis. They enable a foundation that is critical to conducting cognitive warfare, outmaneuvering adversaries in the battle between ideologies, and significantly shortening our OODA loop. In turn, such a foundation can enable and optimize conduct of kinetic action, and enhance the effectiveness of post-competition/kinetic efforts to stabilize an area or region. The greatest challenges to advancing successful future intelligence operations is not our adversaries, their capabilities, access to information, nor technology. **We must understand our biggest hurdles are cultural (policy) and structural (organizational), requiring an overhaul of our production lines and building a new factory floor.**

The BLUF is therefore, we can choose to advance this Future Intelligence Concept of Operations and Future S&T Investment Roadmap 2035-2050, and not only succeed but proactively influence outcomes to match our national security goals and objectives, or we can we fail to undertake these investments and adjustments to advance proactive influence and predictive analysis in the cognitive domain. If we fail to act, we will likely remain in a perpetual reactive posture. The status quo is a losing posture and proposition, guaranteed to see our institutions further undermined, alliances challenged, and military and economic dominance further diminished. If we do not change, we are most likely to end in a cycle of kinetic actions/wars.

There is a kind of dictatorship that can come about through a creeping paralysis of thought, readiness to accept paternalistic measures by government, and along with those measures comes a surrender of our own responsibilities and therefore a surrender of our own thought over our own lives and our own right to exercise the vote. The free system gives the right to every citizen to do something for himself. Because he has the right, the opportunity is always there.

Dwight D. Eisenhower

The Bottom-Line Up Front: We can realize the Future of Intelligence Operations 2035-2050 by understanding that:

- **We must move from a predominately reactive to proactive posture**
 - **We must fight further "upstream" in the information space prior to kinetic action and potentially preventing kinetic action. We are good at killing terrorists or kinetic action. However, we fail to realize that we can't kill an idea. In fact, when we continue to kill terrorists, we often promote and reinforce the adversary narrative.**
- **Technology is not the problem, it's defining the problem.**
 - **Technology is agnostic with respect to the problem. Technology is but an enabler, it is not nirvana.**
- **We are in the midst of a cognitive war, and our focus remains near solely on kinetic**
 - **We can prevent kinetic conflict with a cohesive and well thought out Phase 0 plan.**
- **Our biggest hurdles are cultural and structural, that require new production lines and a new factory floor**

Executive Summary

The views, projections and assessments in this white paper are solely those of the author, and do not necessarily reflect those of the United States Army or Department of Defense.

*We must stop setting our sights by the light of each passing ship;
instead we must set our course by the stars.*

George C. Marshall

The purpose of this white paper is to layout “one” view and projection of what the future of military intelligence will entail in the timeframe 2035-2050. This paper begins with the bottom line up-front, then discusses the four findings, and offers some suggested solutions to address aspects of the findings. The paper moves onto a macro narrative of concepts and projections of a Future Intelligence Concept of Operations (CONOPS) 2035-2050. Several future scenarios provide a projection of threats and operations in that timeframe. The paper wraps up discussing a Future Science and Technology (S&T) Investment Roadmap 2035-2050 and some exemplar technologies likely to advance/impact the future operating paradigm. The roadmap, CONOPS, and exemplars inform and guide an immediate rebalance of investments from a solely kinetic focus to advance capabilities in the cognitive domain. Realizing the narrative and CONOPS, and addressing the findings, requires immediate investments in the new foundation and an overhaul of our current factory floor for both intelligence and defense.

The objective of this white paper is to drive discussion and thought on how we view, use, and integrate intelligence into operations and approaching several paradigm shifts. If we are to realize true capabilities and capacity in the cognitive domain, we must implement a different CONOPS from today. The future intelligence CONOPS laid out in this paper, is intended to inform that effort. We must move to a higher level of integration and collaboration via first a robust whole-of-government, then whole-of-nation effort in supporting the broader defense and national security.

Elements of this paper are likely to be provocative to some and to others in line with similar thinking and discussions. Therein lay a key secondary objective, to drive discussions outside of our comfort zone, cause us to engage in areas we’ve not considered before, and advance a vigorous and cognitive debate on the future of intelligence. In the end, ideas, words and discussion are all intended to advance national security in line with the National, Defense and Intelligence Security Strategies. I tend to shoot for the 75% solution vice perfection. Therefore, this paper is an incomplete product, in the sense that I am limited in time. It is not a thesis but a thought piece.

Serving in multiple roles in the United States Military, Department of Defense, Private Sector and Intelligence Community for over thirty-five years, provides the basis for the contents of this white paper (Appendix B: About the Author). The paper is further informed by inputs, discussions, and engaging over several hundred members of the Federal Government, Private Sector and Academia over the last three years, and in facilitating the efforts of the Army Scientific and Technical Intelligence Community of Interest (Army S&TI COI). I use the word facilitate, vice lead, because we enable information sharing, collaboration and leveraging best practices, key S&T, and capabilities to address specific needs and gaps. We enable and we ask, we do not control nor direct, nor task. The COI’s all-volunteer members are all the true leaders across the IC, DoD and Federal elements. Their participation in our monthly VTC/meeting sessions, numerous other additional forums we’ve hosted, and “speed dating” amongst themselves outside of these forums truly advance their mission and our national security. Thank you to all the COI members for their volunteer participation in advancing this whole of government ecosystem!

The Key Findings Include:

- We must move from a predominately reactive to proactive posture
- Technology is not the problem, it’s defining the problem.
- We are in the midst of a cognitive war, and our focus remains near solely on kinetic
- Our biggest hurdles are cultural and structural, that require new production lines and a new factory floor

The Suggested Solutions Cover:

Addressing the boring, but truly critical stuff, tackles the fact that cultural (policy) and structural (organization) issues are a key problem. Because tackling these issues is often part of “back office” operations, they tend to suffer from attention. They are not glamorous. The likes of General’s Eisenhower and Marshall understood this as their key to success. The section covers three macro cultural and structural issues.

- We need “A New Factory Floor” and achieve this by overhauling and retooling our national security apparatus (DoD and IC). Both the IC and DoD were created out of the National Security Act of 1947, with industrial age processes, that now require a total overhaul in function and structure.
- We need to overhaul and refine our risk and reward system. We must address the root cause of our failure to enable vice control, advance innovation vice the maintain only the status quo, support calculated risk vice over engineering to avoid it, and advance true accountability for actual performance of the enterprise, vice rewarding “titanium cylinders of sub-excellence” that achieve little in output or outcome. We must remove the heavy hand of control, and replace it with the helping hands of enablement.
- We need to overhaul and remake the conscription system & take on new approaches to talent management. We need to move towards acting as an integrated enterprise by advancing a Whole-of-Government (coalition) first, then Whole-of-Nation approach, to address long-term issues related to access to talent, expertise, ensuring recruitment and retention.

The Future of Intelligence CONOPS 2035-2050 narrative and future scenarios project what future operations and events may look like. We all know that few projections survive the test of time. The CONOPS, scenarios and subsequent Future S&T Investment Roadmap 2035-2050 in this paper serve as initial guide for action and investment. The exemplar technologies project areas are likely to have a significantly impact and enable future capabilities. The appendixes offer additional background and insights on the author, the AFC COI (Appendix C: About the Army Futures Command Community of Interest (AFC COI) & Basis and Background for Projections, Findings and Assessment), concept for future analysis, and architecture.

The concerns and thoughts contained in this paper are captured in the below comment, which sums up the murmurs I’ve heard across the IC, DoD and Federal engagements pre and post 9-11-2001.

Unless we adjust our future CONOPS and S&T Investments to account for the paradigm shifts that have occurred under our feet, our nation and its intelligence operations will once again awaken too late, to a different reality, which is likely to end badly with significant and long-term impacts to our nation’s security and place as world leader.

I project such a negative and reactive outcome to occur either because we lost the cognitive war totally, our adversaries succeed undermining our institutions and democratic foundation to such an extent they are no longer viable, or, because our efforts to counter in the cognitive domain came too late.

If we fail to act in the cognitive domain, we will likely end up in a major kinetic conflict resulting in devastating outcomes, in physical and human toll – recovery is questionable.

Edward L. Haugland

Key Findings, Challenges & Solutions

PROACTIVE INFLUENCE AND PREDICTIVE ANALYSIS: MOVING FROM REACTIVE TO PROACTIVE POSTURE

To enable and provide future successful and effective intelligence operations, we must move from a predominately reactive to proactive posture.

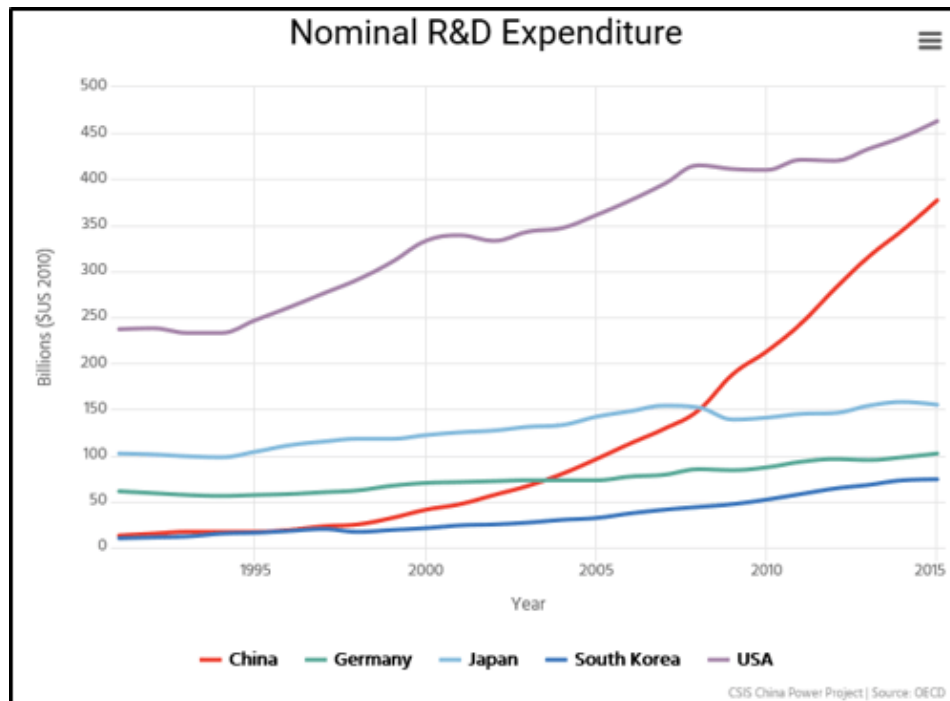
Moving from Perpetually Reactive Posture to one of Proactive Influence and Predictive Analysis:

Our current Department of Defense (DoD) and Intelligence Community (IC) must retool their respective factory floors to move from a highly reactive posture to a proactive posture of influence and predicative analysis. The IC and DoD were created in 1947, during the industrial revolution, to provide indications and warning and prepare for war – in a post WWII Era. For decades the US military and IC dominated in capability, capacity and access to information over private sector, academia, and other governments. DoD and IC R&D investments also dominated those of industry. The industrial age

The only way human beings can win a war is to prevent it.

George C. Marshall

processes and doctrine served us well up until the closure of the Cold War. None of this is true today. In that time period of the late 1980's through today, with the invention of the Internet and explosion of information technology – the paradigm shifted under our foundation. But we did not. The plethora of information and openness of sources from the Internet of Things (IoT), to digital media, social networks etc. now dominates investments in the commercial sector. What we used to dominate, we now try to catchup, understand, and as we do – we've become even more reactive.



Moving to a proactive posture requires an ability to provide actionable information within seconds, from an Army private to POTUS, while ensuring the same relevant common operating picture (COP). It requires an ability to share the same information, or subsets, just as readily with allies, coalition partners or other elements necessary to advance the mission. It requires that we share such data in a manner that ensures our OODA loop is more succinct, precise and clear than our adversaries. Such an operating paradigm is possible today, with today's technologies, but we remain a ways off from realizing

this capability primarily due to cultural and structural relics of how our IC – and as stated in the BLUF – our DoD was originally constructed.

- **Order of 70% of Worlds Research conducted outside of U.S. (to first order, a % of GDP, U.S. produces order of 18% of worlds GDP)**
- **Order of 70% of U.S. Research now “Commercial” (as opposed to Government sponsored)ⁱ**

Moving from a perpetually reactive posture to a proactive posture requires an ability to assess profile and set trip wires for any region and culture worldwide. It requires using information in a totally different manner than most of our current intelligence support is conducted, event to the point where the use of the bulk of information does not initially involve the intelligence community as it now exists. A critical place to start and enable proactive influence and predictive analysis is with the use of public and private information.

There’s been a major shift over the last 30 years. The US government dominating the access to flow of information, R&D and technology is no longer the case. Our IC/DoD no longer controls or owns the majority of information, sensors or other relevant information. Up until the late 1980’s the US government and IC had access to the bulk of unique information and data sets which includes a variety of unique national intelligence information sources. From the late 1980’s on, with the advent of the internet, social media, IoT, etc. – the balance shifted. While the culture in our IC continues to focus on the top secret sources, or moving small bits of open source into a classified domain, our adversaries, private citizens and others can access the 85% solution in seconds either directly from open sources or with a few purchases of data. Furthermore, our industrial age structures and cultures impede our advancement, while our adversaries act with near impunity. We are in a near perpetual state of reaction. It’s time for real change. This requires a commensurate paradigm shift in our concept of operations and future investments if we are to provide a relevant and effective intelligence capability in 2035 out.

The IC’s creation of the term Open Source Intelligence (OSINT), treating such information as a separate discipline, remains a significant impediment to conduct of real-time operations and predictive intelligence. Why? Because the data is usually removed its original state, automatically decreasing its value, then it is pushed up to other security enclaves where it may be combined with other sources, and after some assessment and processing is pushed out to either a very small set of cleared individuals or disseminated via limited bandwidth to military operators, warfighters policy makers, etc.

**“We cannot solve problems by using the same kind of thinking
we used when we created them.”**

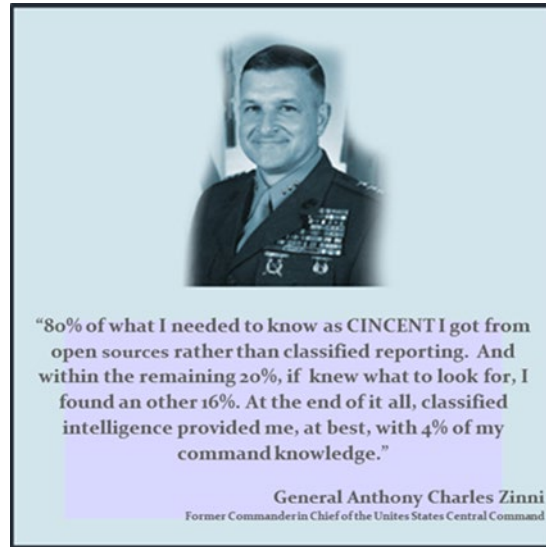
Albert Einstein

Just read any of the OSINT policies or law. Anyone who reads them quickly realizes that there is no quick, easy use, access or sharing of information between intelligence and other operational professionals. Now consider the tactical or operational environment where one needs an instant COP, instant ability to retrieve the latest social media to maintain cognitive awareness of activity in the city in which one is working or operating, and having to move through the bureaucratic hoops and policy laden processes in order to save, share or move the information. Perhaps for those efforts where one has had months or years to prepare, but that’s not the world in which we operate today. We’ve tied our hands, taped our mouths, and watch in wonder how our adversaries act with speed and impunity in the land of the information.

Our adversaries collect, purchase or apply the same bulk open source information and data, assess it and communicate with their elements in seconds of minutes – likely achieving a 85% solution in seconds to inform their decision space. The timelines for their use of information is consistently short in their Observe, Orient, Decide and Act (OODA) loop.

It’s not rocket science, but the IC’s cultural biases to top secret and shunning of open source – or use of it by placing it in another “bucket” called OSINT, places us at a significant disadvantage. Our policies are a major impediment. As once we touch open source (unclassified information) with our “intelligence” moniker – the restrictions on its use are huge, versus unfettered use, dissemination etc. if one were to access the information from home or via their iPhone or droid phone. There are many who will argue we’re increasing our use of open source, that we have an open source center, etc. Correct. However, that doesn’t change the fact that our culture (policy) still remove the bulk of open source information from its resident state, stuff it into a new security enclave or domain, integrate it in order to further assess it etc. and then eventually pass it back to the intended operator or user so they can use it. The end result are delays or the inability to provide a

common COP (from Army private to President), or impede (partial or significantly) efforts to be able to alert in seconds, collaborate in real time in real-world events, etc. If this paradigm doesn't change, our adversaries will continue to out maneuver us in the information and cognitive domain.



The future of intelligence operation 2035-2050 must fully enable use of open source information and provide the 85% solution in seconds, must adjust policy to enable the rapid and free flow of information – not only across US forces and IC elements, but also with our allies and coalition partners. Today's information and distributed ledger technologies (e.g., blockchain) enable the ability to share all, some or specific relevant information in seconds, over current commercial, IoT, LoRa, other networks – and do so in manner that is as or better protective than our current IC networks.

This is not a new endeavor or challenge. I, like many others, have proposed such a paradigm shift in the use of open source for nearly twenty years (Appendix D: Concept 2015, developed and briefed in 1999-2000). The challenges at that time, which remains today, are cultural and structural. Our current approach impedes our ability to quickly enable our operators, disable or impede our ability to engage with our allies, and preclude us from providing a common COP. We need a COP that is readily displayed, accessed (by private to the president), and tailored based to echelon.

We're doing some great things, but we are still operating primarily in a 1947 paradigm. Innovation, information and advantages will flow - if we step outside our boxes. The first step in 2035 CONOPS is changing the paradigm of how we use, assess, disseminate, acquire, etc. open source information – and to stop treating OSINT as a separate discipline, rather treating open source information as it is – true all source information that can be used, applied, etc. for an 85% solution in seconds.

The CONOPS, findings and investment roadmap laid out in this paper, provide a foundation to truly enable intelligence / operations across all phases – competition (gray zone / cognitive domain, kinetic, and post-kinetic). The more pristine the understanding of a region, its criminal, social, economic, political, commercial, etc. networks and players, data sources and infrastructure, and what the respective pain points are, enable an ability to proactively influence outcomes and impacts. Not an easy task. The movement to a proactive posture, proactive influence in the cognitive domain, requires a rebalance of investment from near solely kinetic focus to a balanced portfolio that includes a foundation and tools in the cognitive domain in order to ensure full spectrum of capabilities and options.

The future concept of operations in 2035 includes use of open source to advance an 85% solution in seconds, to out OODA loop our adversaries, and to proactively assess, predict and prevent major incidents while concurrently undertaking proactive influence operations to cause our adversaries to react in ways that benefit our goals and objectives. To enable proactive influence operations and predictive analysis requires a wholly new set of military, political, social, criminal, intelligence, etc. foundation data. The current military intelligence foundation data is focused on targets, facilities, order of battle, etc. While that data is useful in I&W or preparing and conducting kinetic actions, the current military and intelligence foundation data is of minimal use in advancing proactive influence operations or predictive analysis.

Addressing this finding requires movement from reactive posture of preparedness and I&W to that of proactive influence and predictive analysis. Such an effort requires policy and structural changes, and a fuller DOTMLPF assessment.

During this last few years we brought into our COI a few cultural and Internet of Things (IoT) experts that demonstrated real world capabilities using basic technology. These commercial services provide a means to go into any region of the world, and in fairly short order (weeks to a month/few months) layout a detailed COP including pattern of life for that region, the people, cultural mapping, medical, telecommunications, social media, financial, etc. These companies do this work in support of humanitarian efforts or at the request of local governments, to help assess and avoid crises (e.g., agricultural impacts, overwhelming human migration, etc.). The data used is open source from social media, to SCADA, to IoT devices, etc. The COP they created allowed the government sponsor to maneuver resources, military, humanitarian assistance etc. proactively influencing efforts to minimize impacts to their own people, economy, etc. Once such a construct is in place, one can begin to define profiles of activity and patterns of life in a region and use that information to guide action.

However, unfortunately much of the same information is readily accessed and used by criminal and terrorist elements in assessing, acting or influencing their environment or hiding in plain site (e.g., within the normal patterns of activity, commerce, etc.). The 85% solution is available to them, but not presently provided to our own operators in real-time. Why? Because we've not built a construct to provide such information, nor an architecture that advances an understanding of such foundational information and data.

The Secretary of Defense (SECDEF) noted that the use of "Information & Democratization of Technology has changed the Character of Warfare." In addition, in a 2017 SECDEF Memo creating "Information" as the seventh joint function states..."Information is such a powerful tool that it is recognized as an instrument of national power. The advent of the internet, the expansion of information technology...have dramatically impacted operations and changed the character of modern warfare ...the elevation of Information to a joint function impacts all operations and has implications across doctrine, organization."ⁱⁱ

To move to a proactive posture, we must quickly rewrite certain laws and policy dealing with the use of open source information, the ability to conduct influence operations and overhaul the tradecraft, and strongly consider how we can leverage the existing structure (e.g., IC, DoD and Federal agencies) to advance an effort that operates solely in the open domain. We must begin to experiment with ways and means to develop the necessary information foundation to conduct cognitive warfare, enable proactive influence operations and advance predictive analytical capabilities that can support tactical efforts, sustain strategic engagement, and do so regionally based on priorities.

There are many efforts currently underway to advance in this area. They are taking place in the private sector, academia and government. A focused need or gap may be the primer, to create a burning platform, to begin to change and coalesce the many efforts into a focused approach. Strategic design is but one method to consider in tackling the next steps related to this finding.

"Strategic design differs from planning not only in its strategic context, but also in purpose, methodology, and output. Unlike plans, which attempt to script out a sequence of actions, strategic design should aim to comprehensively and continuously understand the problem. Such a strategy should remain above the level of operational detail, and instead convey a grand, system-level, conceptual overview. It should provide an orientation to the commander's understanding and intent, like a compass bearing that points toward desired or acceptable futures. From this understanding, subordinate operations can be devised and executed, via delegation and the principles of mission command."ⁱⁱⁱ

TECHNOLOGY IS NOT THE PROBLEM, IT'S DEFINING THE PROBLEM

Information & Democratization of Technology has changed the Character of Warfare. We must understand that technology is not the problem, it's defining the problem.

Technology is Not the Problem – Its Defining the Problem: We continue to fail to focus and define our problems in simple, easy to understand terms. We also fail to provide insights into the work that is already taking place. To fully enable the benefits and exceptional capabilities of the private sector, academia and collaboration/synergy among government, we need to clearly define our needs in simple terms, provide some level of insight into what we're already doing and status. These two basic sets of information can help to avoid an extremely wasteful and costly guessing game, inform investments and development of capabilities, and advance real competition (in and outside of government) to find the best, most cost effective and timely solutions from academia, the private sector and within the federal government.

Yes, we must balance access to such information and protection of our national security – but our culture that's developed around our acquisition processes over the last several decades continues to grow in complexity and the number of hurdles of entry in a manner that limits our access to ideas, concepts, and diversity of thought and input. Yes, there are efforts underway, but it's time to retool that factory floor.

We must begin by focusing on a piece of the elephant (using a metaphor), rather than trying to eat the whole elephant. In addition, we must clearly define our problems/needs in simple terms – that do not hint at either material or non-material solutions. During the first two years of our Army S&TI COI, we were not able to get the Army elements to focus on a small subset of needs. Thus, our engagements with the IC, DoD and other Federal organizations were less fruitful – as their inputs tried to cover the elephant.

This last year, 2018, in most part thanks to the Army's Chief of Staff and stand-up of several Cross Functional Teams, we were successful in narrowing our focus to seven enabling intelligence function needs/gaps. The last year demonstrated, once we defined a set of priority needs/gaps (a piece of the elephant) the inputs from our COI, external organizations, technology scouts, etc. were tremendous. We received inputs during our monthly VTCs/meetings, from our own technology scouting efforts, other technology scouting efforts from across the DoD, DIU, InQTel, several IC agencies and more. The challenge remains in being able to sift through those inputs fully to assess their application against the needs/gaps, and mapping them to a Future S&T Investment Roadmap. In other words, technology was not the problem. I believe there are multiple potential current technologies that can resolve the defined needs/gaps 25% to greater than 90%. What was missing, were clear, simple, focused definitions of the need or problem.

An essential part of any successful action on the part of the United States is an understanding on the part of the people of America of the character of the problem and the remedies to be applied. ... It is virtually impossible at this distance merely by reading, or listening, or even seeing photographs or motion pictures, to grasp at all the real significance of the situation. And yet the whole world of the future hangs on a proper judgment.

George C. Marshall

An organization that serves as an exemplar in defining the problem in simple form is SOCOM. Their S&T element regularly puts out new needs in simple, easy to understand, 8th grade English. From discussions with their team, we found that anytime they prepare a new requirement, they take the draft and pass it by a couple of their interns. Many of the interns have little to no military background, and are usually just completing their academic years or early in their private sector career. This type of review serves to make the problem set understandable to a much wider audience and avoid inserting information that includes non-material or material solution hints or directive language.

Defining the problem in simple terms also lends itself to discussing, understanding and obtaining inputs from other IC, DoD and Federal elements. The current tendency is to define the problem using a solution set that includes a material solution example. Such an approach can impinge upon an open dialogue, result in unique options not being considered, limit potential solutions due to misperception, and truly limit consideration of traditional or unique possibilities.

Additionally, current approaches to defining and solving the problem can be, and most likely are, significantly hampered by an inability (even in and among government only circles) to understand the state of the current program or capability, what investments are being applied to the problem, and obtaining insights into the status of the program or investments. I refer to the barriers in obtaining such insights and understanding as the “Charlton Heston Effect.” For those that can remember, one of Mr. Heston’s post acting careers most famous moment was when he held a rifle in the air and stated “I’ll give you my gun when you pry (or take) it from my cold, dead hands.” Trying to gain insight into current programs of record, S&T portfolios, or other projects in our federal space – seeking information on status, funding, options, etc. – one will usually run into a number of obstructions –the “Charlton Heston Effect,”^{iv} One is not likely to get much information out of the program, PEO or project manager without prying it from them. This cultural issue is addressed later in this paper, as it relates to our current system of risk and reward. However, as we fleshed out the Future S&T Investment Roadmap in 2018, we did find enough program managers, a few PEOs and a few project leads willing to share insights – as they provided those insights in response to the designated needs/gaps during our Army S&TI COI sessions. The COI, as it continues under AFC, can benefit as it has the authority to direct inputs from Army elements, thus avoiding the “mother may I” approach. AFC is not likely to avoid the Charlton Heston Effect – at least not in the near-term.

Having not only a clear problem statement, but insights to a number of potential programs, projects, etc. (across the IC, DoD and Federal) that could be applied partially or in whole against a specific set of needs/gaps, truly opened up the opportunities for leveraging best efforts, practices, and other investments to advance solutions, shorten acquisition timelines, or decrease costs. The degree of cross-pollination that occurred outside our COI was tremendous. Sharing proposed solutions, against a small and clearly defined set of needs/gaps, with a common framework and template (**Future S&T Investment Roadmap picture**) – provides a portfolio snap shot.

Article: Leap-Ahead Technologies: Could They Be the Army's Undoing?

By Matthew Cox, Military.com, April 29, 2018

In Scharre's opinion, the Army's modernization effort should not be aimed at replacing all existing ground vehicles with new platforms.

"If I were to rack and stack Army modernization priorities, I would not focus on ground platforms at all," Scharre said. "Because the underlying technology to make a tank has not radically changed, so we could spend billions of dollars and come up with a tank that is marginally better than an existing Abrams." Army generals do seem to be very aware of the past mistakes the service has made with modernization efforts, and not just with FCS...

Gen. Stephen Townsend, commander of Training and Doctrine Command, said the service has attempted to improve the way it equips individual soldiers and squads more than once over the past 27 years...

"Since 1990, there have been no fewer than three efforts that were undertaken by our Army a lot like this one, using almost exactly the same language -- Soldier as a System, Ground Combat Soldier System and something similar to that," he said during a panel discussion at AUSA on the Soldier Lethality priority...

"They used the same language we are using today; the goal was to achieve decisive overmatch at the soldier and small-unit level," he added. "Here is my point: Fifteen years from now, I hope my successor is not sitting here showing you another version of my slide, talking about the importance of this topic and why we haven't got it right yet.

Paul Scharre, a senior fellow at the Center for New American Security.

What we also found in this approach, was that while the initial needs/gaps were Army centric – they were 80-85 percent similar to other DoD, IC or Federal needs/gaps. We need to approach the problem differently, with a different discussion. The above article speaks to this issue, while also reinforcing the definition of insanity^v.

The optimal next step, which we were not able to complete in the first three years, would be engaging academia and private sector using the inputs we've received via our COI's "whole of government" effort. Using those inputs, one could engage in a unique discussion and engagement with private sector and academia by providing them a clear understanding of the needs/gaps, insights into what the government is already doing (portfolio view), while putting the efforts into a simple and easy to understand context – the roadmap format. The other unique variable in discussions would be to focus not so much on the business development elements, but on inviting and engaging with actual private sector and academia S&T, engineers, concepts people and architects. The intent is to bring the two-person startups to the big companies and provide them: A) An opportunity to talk to user/owner of the need/gap to gain insight and understanding of the problem set. And, B) Provide a macro summary of the Future Investment Roadmap of what the government is already doing (that which the government is willing to share) so they not only understand the need/gap but efforts underway.

With that context, the government would be able to ask our private sector and academia for their input/feedback along three lines: 1) What could they offer in capability, process or other ideas to move current schedules to the left? 2) What could they offer that would support meeting a need/gap faster, better, lower-cost with ready capacity/capabilities? And just as critical open up the dialogue by asking them. 3) What are we missing, should consider, or are not even considering? It's a dialogue that rarely takes place, provides a truly level playing field for the startups to large companies, and provides a better understanding of where potential IRAD investments could be most optimal.

WE ARE LOSING THE COGNITIVE WAR, WHILE FOCUSING NEAR SOLELY ON KINETIC

Our biggest challenge, is that we are in the midst of a cognitive war that will last a millennia or longer, and our focus remains near solely on kinetic.

The primary finding, and our biggest challenge I contend, is that we are in the midst of a cognitive war that will last a millennia or longer, and our focus remains near solely on kinetic and technology. While we must endure and prepare for overmatch if faced with a kinetic conflict, we are losing multiple and significant battles daily in the cognitive realm.

Whether it's the continued theft of our technology with little retort, avoiding and countering efforts to undermine of our democratic institutions from a variety of foreign actors, an inability to counter false narratives of communists or dictators that continue to preach the failed ideology of socialism/communism, or failing to advance a broader whole of nation understanding that our democracy, freedoms, opportunities and way of life are not guaranteed – and are under attack via many fronts that have torn at the fabric of our democracy. We in the United States of America fail to have a cohesive and prescriptive strategy laying out milestones and objectives in the battle of ideology. We remain reactive. We need to develop clearly defined strategies for each region of the world to advance the human condition, principles of freedom, capitalism and democracy.

POLITICAL WARFARE is back, and the United States is losing. As great-power competition has intensified in recent years, China and Russia have undertaken multi-pronged offensives to undermine American influence and erode the U.S.-led international order. These offensives have included defense buildups, geoeconomic initiatives, paramilitary coercion and even (in Russia's case) outright military aggression. They have also featured determined political warfare campaigns.

<https://nationalinterest.org/feature/how-wage-political-warfare-38802>,
By Hal Brands Toshi Yoshihara, Dec 16th, 2018

Of these findings, this will likely be the most provocative and controversial. The future of warfare is critically dependent on our ability to fight and win in the cognitive domain. The application of technology and information in the cognitive domain is primary path to successful outcome no matter the objectives. The ability to temporarily subjugate people, or nations, via kinetic or forceful means will remain a constant.

However, when taking an historical and future perspective, to sustain long-term US national security interests requires influencing and winning in the cognitive domain. At present, the US our DoD and IC are ill equipped to act or win in this domain. Our adversaries are using multiple paths in this domain to out maneuver us to achieve varied successes. We refer to these activities as occurring in the competition phase, or Gray Zone operations, Influence, PsyOps, etc. Nonetheless, they are all aspects of competition in the Cognitive Domain. As the power of the pen, the idea, the thought to influence is primary – whether those ideas, thoughts, etc. are real, propaganda, etc. are another matter. But our adversaries, primarily the Chinese and Russians are using varied methods in the cognitive domain to undermine our alliances, steal our technology, subvert our democratic institutions, etc.

Despite these glaring realities, we remain near solely focused on advancing kinetic solutions. Our adversaries know that direct kinetic action is not likely to produce a favorable result. Their use of varied tactics, techniques and other in the cognitive domain will, if unanswered, preclude the need for or significantly reduce the need for kinetic action. Kinetic capabilities can dictate an outcome, but sustained long-term outcomes will remain solely dependent upon the ability to influence, affect, change, or impact the cognitive domain.

The cognitive war, is a mostly hidden war, because it rarely involves direct confrontation or kinetic action. It involves a war of ideologies. China and Russia remain the primary threats in the cognitive domain. If we fail to not only counter punch in this domain, but build a sustained and proactive foundation to advance in the cognitive domain, we will have no other option then an eventual kinetic conflict. Engaging in the cognitive domain requires moving from a perpetually reactive posture to advancing proactive influence operations and impacts that require our adversaries to react. By engaging in the

cognitive domain, we can not only avoid most kinetic options, but remove ourselves from a perpetual cycle of conflict in certain regions of the world. Operating in the cognitive domain covers several areas previously viewed as distinct areas—whether psychological operations, information operations, civil affairs, etc. A broad area announcement (BAA) from United States Army, Communications-Electronics Research Development and Engineering Command Intelligence and Information Warfare Directorate (BAA I2WD 2014, Formally Solicitation Number: W56KGU-14-R-0003) viewed information operations in the following manner:

Information Operations (IO) elements include synchronized Computer Network Attacks (CNA)/Computer Network Defense (CND), Psychological Operations (PSYOP), Military deception, Electronic Warfare (EW), Special Information Operations (SIO), Physical destruction, operational security, counterpropaganda, counter-deception, physical security of Command and Control (C2), Information Assurance (IA), Counterintelligence (CI), and related activities, such as Civil Affairs (CA) and Public Affairs (PA). Using CNA, PSYOP, military deception, EW, SIO, physical destruction, and other capabilities, IO can be used offensively to influence ideas, perceptions, beliefs, decisions, and communication of information of enemy. Using IA, CND, PSYOP, military deception, counter-deception, EW, and other capabilities, IO can be used to defend decision-making processes, by neutralizing adversary perception management and intelligence collection efforts, and attacks on our INFOSYS. IT-based tools will increase U.S. Army Commanders' IO capabilities and combat power. Examples of such tools include the Internet, global broadcast television, network attack techniques (corruption of data or Denial of Service (DoS)), electro-optic, electromagnetic, high power radio frequency, audio, and seismic weapons; special purpose/multispectral obscurants, advanced INFOSYS and network security, and 'intelligent agents'.

It requires a set of skills, foundation, infrastructure, capabilities that partially existed during the cold war. It requires a broader strategy and whole of nation approach on par with our adversaries with one major difference – our strategy must leverage the individual strengths, will and patriotism of our people and government, private sector and academia institutions working together in the cognitive domain vice being directed, controlled, or threatened by fear of punishment or worse. And, to be truly successful, it requires partnerships with our allies and other coalitions worldwide.

Our focus, and that of the National, Defense and Intelligence Security Strategies, are on a set of threats – that continue a pattern not unexpected from a historical perspective – that mixes near-peer advances in kinetic, technology, and proxy capabilities with the spread of radical terrorist groups continues unabated. However, the battle for humankind has always been a primarily cognitive one. Even today, the primary threat ebbs and flows from those who would control, subjugate or destroy civilizations to advance their power, ideas and intent (like China, Russia, Iran, Cuba, etc.) to those who would rather advance civilization by enabling freedom, opportunity and independence (USA and our allies).

The cognitive domain brings broader challenges in that it requires a strategy that can last beyond our political election cycles to enable a long-term sustained and proactive means to influence and impact others in order to affect change that advances our ideals. Our nation faces a variety of threats from near-peer, to those sponsored by nation states, virtual nations and spanning to long-wolf actors that aligned with a variety of ideological, religious or other beliefs that motivate their cause and actions.

Unless we begin to undertake proactive operations in the cognitive domain, align our government institutions, and restructure our intelligence apparatus to enable such proactive operations, we will remain solely on a path of two choices. One path will allow our adversaries to undermine us from within/externally – thus avoiding kinetic but having lost our basis for democracy. The other path, we will find ourselves with no other option than direct kinetic confrontation in which we may or may not have overmatch. In today's world, as the national security strategy points out, we no longer have sanctuary and therefore any major kinetic action is likely to have such major negative impacts on our nation that recovery will be questionable.

The efforts of our adversaries in the cognitive domain is unending and with little response. It is time that we realize the paradigm has not changed from the cold war era with some countries, and that they continued to expend efforts in the cognitive domain while we took a peace dividend. We must move towards operating as an integrated enterprise, whole of government, then whole of nation.

Our ability to respond to challenges in the gray zone, cognitive domain, requires that we integrate across our titanium cylinders of sub-excellence, and become an integrated enterprise – by service, by department and across government. Once we begin to figure that paradigm shift out, and perhaps the new efforts in standing up a space force can facilitate such integration, then we'll have a fighting chance. It's time to update our doctrine and our factory floor while realizing our

future is in a whole of government/nation enterprise. The RAND Corporation just finished a report on Russia's hostile measures – and one of the two key findings is that they are conducting hostile measures short of war. Their recommendations buttress the findings of this paper. However, the findings and proposed approaches in this paper go well beyond the recommendations by Mr. Raphael Cohen and Andrew Radlin^{vi}

Russia's Hostile Measures in Europe: Understanding the Threat
Raphael S. Cohen, Andrew Radin, www.rand.org/t/RR1793

KEY FINDINGS

Hostile measures are measures short of war

- The term hostile measures encompasses a wide range of political, economic, diplomatic, intelligence, and military activities that could be perceived as harmful or hostile.

RECOMMENDATIONS

- In deploying forces to Europe to counter Russian aggression, the U.S. Army should also prepare to defend against and counter Russian hostile measures. The Joint Force and the Army must also consider how Russia might respond aggressively to any forward-deployed forces.
- The U.S. Army should develop counterintelligence, public affairs, civil affairs, and other key enablers to better counter Russian hostile measures.
- Responding to Russian hostile measures places a new premium on political awareness, as well as on crisis management. U.S. military personnel need to be aware of Russian hostile measures—particularly when deployed in countries with frozen conflicts or where there is a large pro-Russian population—to help avoid accidentally sparking a crisis.
- Whatever the U.S. response, preparation for involvement in a wide range of conflicts can help reduce the risk of mismanagement, miscalculation, and escalation

We must expand what were traditional Special Operations Force (SOF) capabilities and scale them into the general force, but broaden their integration with whole of government effort so that SOF can remain focused on the tactical but we can enable strategic engagement in the cognitive domain.

...it is SOF's ability to operate jointly at the tactical level to influence the human domain for strategic and operational effects that truly sets it apart. SOF's broad range of missions dictates the need for small, purpose-built task forces consisting of ground, maritime, and air elements optimized to engage in the irregular, population-centric conflicts occupying the contested space between war and peace. This space, known colloquially as the Gray Zone, has become the focus of SOF's recent efforts against terrorism and insurgency across the globe and has increasingly defined its *raison d'être* when compared to conventional forces^{vii}

Future intelligence operations will enable success in the cognitive domain. However, to achieve superiority in the cognitive domain requires an immediate rebalance of current investments to provide a totally new information foundation, refining or removing policy barriers to sharing of information, and providing a robust architecture to rapidly share that information. Providing for immediate and proactive deployment of that infrastructure requires a new means of communication and new varied sensors/capabilities to capture new information sets. Such activities will provide a sustained means to conduct and enable proactive influence operations and advance predictive analysis. Advancing proactive influence operations and predictive analysis to win in the cognitive domain requires new expertise, reviving old tradecraft, and advancing new levels of integration towards a whole of government/nation approach to national security.

The good news is that the means, technology and information to achieve such capabilities are readily available in today's commercial markets. The investments and capabilities realized in-turn provide an absolutely critical foundation to winning any kinetic conflict. This foundation also serves another critical purpose – achieving success in post conflict (kinetic or other) efforts towards ensuring sustained peace. Developing these capabilities, foundation and expertise requires a sustained national effort, now through 2035, in establishing the baseline capability that will upset the dynamics of our adversaries, causing them to react to our efforts.

We need a broad and in-depth strategy for influence operations and predictive analysis. We are in a cognitive war, and it is a war of a millennia, not years, decades or centuries.

**Wars are bred by poverty and oppression.
Continued peace is possible only in a relatively free and prosperous world.**

George C. Marshall

Just as important as leading the necessary changes in acquisitions, we must not forget, it's not all material. We are losing the on-going war. We have no game plan for the cognitive war. It is the never-ending competition in the Gray Zone that will make kinetic action OBE, unless we immediately rebalance our investments, interest, and efforts. The National and Defense Security Strategies both speak to this challenge and accelerating multi-domain operations. The article in the below link (Accelerating Multi-Domain Operations, Evolution of an Idea; by Gen. Stephen Townsend, U.S. Army, Article published on: 8 August 2018) does a great job in laying out the case for joint operations, leveraging broader coalitions and understanding that efforts entail more than just the fight.

<https://www.armyupress.army.mil/journals/military-review/online-exclusive/2018-ole/aug/accelerating-md/>

There are champions across the DoD working on these challenges. From the SOF world and SOCOM, to OSD SOLIC, USD(I), the Joint Information Warfare Operations Center (JIWOC), etc. One of the key foundations is policy. The Joint Chiefs of Staff and the Office of the Secretary of Defense Policy are, among the others, working hard to address this issue. OSD has issued the Strategy for Operations in the Information Environment (SOIE), and Joint Concept for SOIE. They can be found at: <https://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/>

My take, these are foundation documents that DoD and federal government must place as one of our highest priorities. The SOIE gets the basics right, while asking for the plans. Our adversaries are winning the 3rd world war - which is an information, ideological – or cognitive war. The SOIE and JCOIE give us a start and next steps in moving to overcome significant disadvantages. They are only the first steps, and require a concerted effort that is inclusive of a broader set of diverse SMEs.

There are also a number of efforts underway across the government, private sector, and academia to address the challenges in the cognitive domain. The following extracts from articles/publications provide some great insights into some efforts and discussions underway that begin to address operations in the cognitive domain and social networks, the use of “sharp power,”

United States Institute of Peace; Soft Power in a Sharp Power World: Countering Coercion and Information Warfare: A Bipartisan Congressional Dialogue with Rep. Francis Rooney (R-FL) and Rep. Don Beyer (D-VA) Wednesday, November 28, 2018

Sharp Power: The New Threat -- Soft power, the appeal of a country's culture and values to enhance its strength and influence, has a new foe in “sharp power.” As employed by global adversaries like Russia and China, sharp power utilizes information warfare techniques through media initiatives, cyber activities, and cultural exchanges to achieve geopolitical goals and weaken Western influence. Russia's efforts to subvert the liberal world order and undermine global norms by interfering in democratic processes at home and abroad provides a salient example of sharp power at work. Beyer said he worried that beyond the inherent dangers of the technological tools of global adversaries, America's declining soft power around the world makes it even more vulnerable to sharp power. In order to reassert and maintain its power, both congressmen acknowledged that all forms of power are necessary components of statecraft, but maintained the importance of employing soft power tools. Three critical components to American soft power are: “Our cultural exports, our economic preeminence, and the power of the American ideal....To counter sharp power with soft power, Rooney urged the U.S. to refocus on its values and culture, its symmetrical and reciprocal alignments that “allow everybody to win,” and build on multilateral trade relationships. He and Beyer both underscored the importance of USAID, cultural exchange programs, and the U.S. diplomatic corps.

Visualizing Social Networks to Inform Tactical Engagement Strategies that will Influence the Human Domain Molly MacCalman, Alexander MacCalman, Greg Wilson; Small Wars Journal, August 15, 2013

The Special Operations Command, Marine Corps, and Army recently formed the Strategic Landpower Task Force to study the confluence of the land, cyber, and human domains. To support the Task Force's research, this paper demonstrates the utility of visualizing social networks in order to inform a unit's population tactical engagement strategy.

The human domain is one of the most critical and challenging aspects of modern conflicts and will remain a decisive factor in future conflicts. A recent white paper signed by key military leadership states, "Time and again, the U.S. has undertaken to engage in conflicts without fully considering the physical, cultural and social environments that comprise what some have called the human domain." [i] In order to prevent, shape, and win future conflicts our forces must embrace the challenge of understanding and influencing the human domain. To address this challenge, a new partnership between the Special Operations Command, Marine Corps, and Army has recently chartered the Strategic Landpower Task Force to study the confluence of the land, cyber, and human domains. [ii]... Although the methods of social network and link analysis are not new to the military's analytical community, the challenge of collecting the right data in the right structure makes these methods difficult to apply at the tactical level....The physical, cultural and social environments that encompass the human domain involve complicated dynamics among people and organizations. Understanding the human dynamics of the regions where our forces are deployed is essential to preventing and containing future conflict. Some examples of these dynamics include the disequilibrium of power, social inequities between ethnic or tribal groups, intimidation by insurgents, government corruption, and lack of essential services and wealth generation mechanisms.

Influencing these human dynamics requires a comprehensive effort to increase our understanding of the population's key influencers and social structure...To conceptualize the human domain we can leverage models of human networks that illuminate the interconnected socio-cultural structure of government officials, local nationals, insurgents, other hostile elements, Coalition Forces, and other state and non-state actors....Identifying potential communities that share common social ties can assist units to address local disputes, build consensus, and disseminate information...The social structure in a sociogram implies an inherent flow of information or resources through the network. The unit can find actors that lie on the shortest path between pairs of actors and exploit these broker positions or bridges by manipulating the information or resources that flow through the network'.

By SYDNEY J. FREEDBERG JR. on December 07, 2018 at 4:00 AM

Army Multi-Domain Update: New HQs, Grey Zones, & The Art of The Unfeasible

<https://breakingdefense.com/2018/12/army-multi-domain-update-new-hqs-grey-zones-the-art-of-the-unfeasible/>

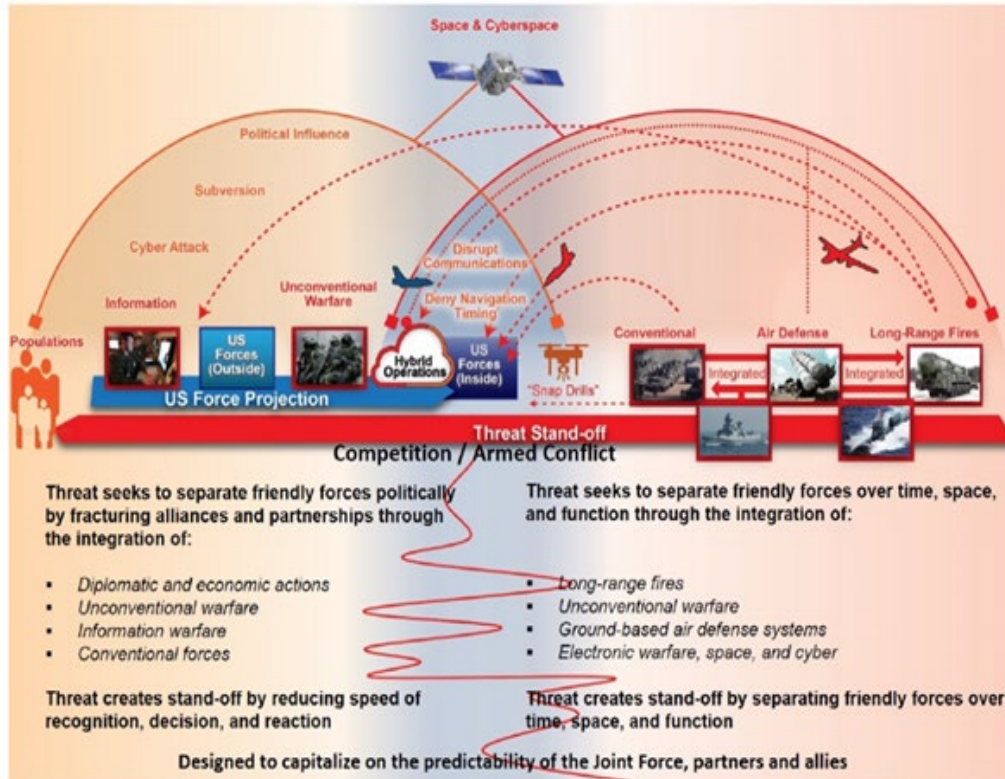


Figure 2-2. China and Russia in competition and armed conflict

The Gray Zone

The most obvious change is the name, but it's more than just words. The Army's shift from Multi-Domain Battle to Operations was meant to broaden the focus from just fighting — tactics — to a wide range of operational and even strategic concerns. Today's document backs this up with extensive sections on what the Army must do in "competition," the "gray zone" between peaceful cooperation and open war, in which authoritarian and adaptable adversaries like Russia and China pursue their goals aggressively but not violently through everything from propaganda to proxies to military positioning.

Yes, "competition" featured in the Army's October 2017 Multi-Domain Battle paper and in Defense Secretary Jim Mattis's January 2018 National Defense Strategy. But this latest Army concept gives competition more depth and emphasis, elevating it beyond mere preparation for war and "shaping the theater" to the Army's primary mission:



SOURCE: Military Review, December 2017.

Article Continued. By SYDNEY J. FREEDBERG JR. on December 07, 2018 at 4:00 AM

Army Multi-Domain Update: New HQs, Grey Zones, & The Art of The Unfeasible

<https://breakingdefense.com/2018/12/army-multi-domain-update-new-hqs-grey-zones-the-art-of-the-unfeasible/>

...“The central idea is the rapid and continuous integration of all domains of warfare to deter and prevail as we compete short of armed conflict,” the document says prominently (boldface in original). “If deterrence fails,” it continues, then the Army engages in armed conflict to “penetrate” enemy defenses, “dis-integrate” them (the hyphenation is deliberate), “exploit” the resulting weak points, and “consolidate gains to force a return to competition on terms more favorable to the US, our allies and partners.”

“It’s a recognition of the reality that we’re in competition all the time,” said Gen. Stephen Townsend, who as head of Training & Doctrine Command (TRADOC) is Lt. Gen. Wesley’s boss until mid-morning Friday, when ARCIC transfers to Futures Command.

War on the Rocks, The Will to fight and The Fate of Nations, Ben Connable and Michael Mcnerney, Dec 20,2018

The Problem: American Military Reluctance to Embrace Human Complexity

Understanding human behavior is difficult. There is a powerful American cultural imperative to view war primarily as a mechanical problem. The human element is held aloft in military history, theory, and doctrine, but it is too often downplayed or ignored in practice.

America’s military services typically view war as a contest of opposing, independent gear. Some present American conceptualizations of war as redolent of the worst excesses of the “revolution in military affairs.” In this aspirational and pristine vision of modern warfare, tanks fight tanks and planes fight planes in an anthropomorphic clash of metal. Technology and comparative tables of equipment dictate official predictions for wars’ outcomes.

This dynamic may be most obvious in military war games and simulations. Most are bereft of the human element. Simulated soldiers march sharply into withering enemy fire, obeying even the most reckless orders without hesitation or deviation. This gives war games and simulations a glossy veneer of mechanistic neatness that all but ignores historical experiences with warfare and human behavior. The breaking of the adversary’s will is rarely a central design consideration....U.S. Army Special Operations Command recently proposed the concept of cognitive maneuver. Their central argument is that the joint force needs to “maneuver toward cognitive objectives,” which means finding ways to change human behavior by changing minds through a tailored combination of force and influence.

OUR BIGGEST HURDLES ARE CULTURAL (POLICY) AND STRUCTURAL (ORGANIZATION)

We must understand our biggest hurdles are cultural and structural, requiring an overhaul of our production lines and building a new factory floor.

The Biggest Hurdles are Culture (policy) and Structural (organization). This finding is likely not alarming, nor controversial. It's sort of like talking about the elephant in the room, that obvious problem that everyone sees, but few wish to point out. Why? Because the tendency is to try to tackle the elephant in whole, and in doing so, the elephant typically responds by pushing back and squashing those tackling it by firmly sitting down to maintain the status quo.

Typically, fixing cultural and structural issues are viewed as having to take years or decades. Many view sloth like progress as success. I believe that thinking such efforts have to take so long is a false premise. If we adjust our approach, take on the challenge by taking a bite of the elephant, chewing on it, and digesting it one piece at a time – the likelihood of success increases. Nothing says we can't invite others to the party and have several take a bite at the same time. Such an approach tends to forgo long delays, refinements, or adjustments and advance more rapid and successful change.

Culture = Policy + People + Process

Edward L. Haugland

Culture = policy + people + process. Once each of these areas is defined, if there are issues, they can be addressed. Once the policy is laid out, the key is to determine the processes needed to enable fulfillment of the policy in order to deliver the desired product or outcome. The people, for example various types of expertise or skill levels, are then assigned to implement a part of the process in line with the policy. Accountability is achieved by monitoring implementation of the policy, via the processes involved, and determining what is working, what's not working, and adjusting, refining, replacing etc. until policy, process and people produce the desired deliverable or outcome. In doing so, a culture is created. If any of the three key elements aren't working properly (i.e., policy, process, or people) then each element can be refined, replaced, or in the case of people retrained or reallocated to other priorities until one achieves desired deliverable or outcome. The culture matures and is advanced via accountability.

While form should follow function, the tendency in the federal bureaucracy is to define the boxes first and then force fit the functions into a preconceived notion. In other words, the tendency is to layout the structure of an organization along the lines of current perceptions and practices, despite a desire to deliver something new or achieve something different. Then leadership is usually amazed or confounded as to why the structure is not working. Sort of like a company making tennis shoes for years, now wanting to make automobiles, and doing so by adding a few more people, squeezing in a metal shop, adding a new sign to the front of the factory, and then wondering why cars aren't coming out the other end – but rather tennis shoes in metal shoe boxes. Sound familiar.

Once form follows function, and the structure properly aligned – the application of policy, people and process (Functions) can more readily be implemented, adjusted and refined. The cultural changes an agency, office or business desires are achievable, and in short order, if one understands this simple construct. The suggested areas for improvement that follow provide additional details. Changing out a factory floor/retooling it (i.e., structure = organization) and adjusting the culture (i.e., policy + process + people) can be achieved rather quickly in months to years, vice years to decades, if properly planned “up front.” However, the tendency in government is to address piece parts of the whole, and not address the whole (e.g., the “enterprise”). In doing so the interdependencies, external dependencies, etc. are not typically thought through. We therefore tend towards slowly adjusting the structure or culture, and do so in a manner that extends the timelines, to achieve a desired deliverable or outcome. The premise being that cultural and structural change takes decades. I contend that's a seriously wrong premise.

The absence in understanding is not too shocking, given most of our leadership and people are trained, focused and rewarded based on supporting their piece of the enterprise, not the enterprise. This is a fundamental flaw. Without tying efforts to the success of the enterprise, expanding our “play book” to leverage the fuller set of playbooks available across the

federal enterprise, the system can become warped. Such a construct are remnants of industrial age processes. Albeit, in certain functional areas of businesses they still add value. This is not necessarily the case when applied to intelligence or defense. Such practices worked fairly well through early 1970's, but I believe began to wane in the 1980's and more so with the advent of the information age and rapid advances of technology.

The reward and risk system for most of the last sixty-plus years, living off of an industrial age mentality, to include today rewards the most not for what is achieved or produced, but for what is controlled (e.g., people, information, programs, dollars). The current structural and cultural norm is to focus on individual silos. This was a good thing in the past, but with the challenges faced today, we require increased collaboration, flow and sharing of information, leveraging between programs, and ensuring integrated, redundant and survivable enterprise constructs that rely not just on whole of government, but whole of nation constructs. Our adversaries (peer or near-peer dictatorships) are advancing whole of nation approaches.

However, what's typically missing is an "enterprise" perspective that also takes into account how the efforts in each of the silos are or are not advancing the value and understanding the enterprise. Hence, we find many "titanium cylinders of sub-excellence." The new Army Futures Command is being stood-up, but it remains unclear how this piece of the enterprise fits into the rest of the enterprise. It remains unclear how this new piece of the "factory floor" is intended to operate within the confines of the greater factory (the Army Enterprise) and how it engages external elements (greater joint enterprise).

The initial piece parts of AFC are placed into a structure that addresses the upfront portion of the factory floor (i.e., pilot, prototype, exercises, to requirements). Nevertheless, there remains a lack of clear alignment and integration with the fuller enterprise functions through acquisition, updating technology during the lifecycle, etc. As such, it is hard to understand the linkage between internal or external (e.g., joint) elements/functions or readily explain to others what the key inputs, outputs and desired outcomes are – from the "enterprise" perspective. This leads to confusion, impedes input and support, and enables those who wish to sustain the old factory floor (i.e., demonstrate passive aggressive tendencies). Either way, the development of the new factory, structure and culture desired is extended.

Dr. Griffin/OSD R&E addressed the need to adjust our bureaucracy in an 8 June 2018 *Breaking Defense* news article (captured below). The inability to understand the enterprise and its architecture is not surprising given the continued tendency to focus on our "titanium cylinders of sub-excellence." We must begin referencing our macro enterprise architecture – which consists of the vision and strategy, the resources to implement, and the core functions (i.e., ends, ways, and means).

...Griffin, who took office in February, has blasted the Pentagon's slow-moving, risk-averse culture, saying "my greatest enemy is time; my greatest enemy is not breaking a piece of hardware" in testing. He said recently that his message to Mattis has been that, "we can either retain our national [military] preeminence, or we can retain our processes, but we cannot have both. We have to thin out our processes like weeds in your favorite garden...

If you wish to succeed in implementing a strategy, one must tie the ends (vision/strategy), with the ways (functions), and means (resources). That requires some consideration of what the outcomes and deliverable are required, the functions needed to produce those deliverables, and the type of resources required to enable. If the cultural and structural elements are not well laid out, the resourcing is likely to not make much difference. Alas, we continue to make this mistake. Every commander and every leader should understand, be able to define, and clearly delineate the Minimal Essential Architecture (MEA) required for success (ends, ways, means and how they fit together). If they cannot, why would you expect success? This applies in war, competition or peace (Appendix E: Enterprise Architecture Depiction)

CHALLENGES & SUGGESTED SOLUTIONS

Addressing the Boring – But Truly Critical Stuff

Dealing with these challenges does not require a degree in rocket science. It is dealing with fundamental management cultural (policy), structural (organization and process) issues – that which many managers consider to be the “boring” stuff. Cultural and structural elements are often perceived and dealt with as third order in importance, useful but not drivers, and are typically displaced in priority by the crises du jour of the moment. They are viewed with disdain, boring, and back office administrator functions. In fact, they are the critical elements enabling effective and efficient implementation of strategy via linkage of the ends, ways and means. The genius behind the successes in WWII was General’s Marshall and Eisenhower’s proactive efforts and focus on the “boring” stuff (i.e., logistics, manning, training, industrial base, etc.).

Most things which are urgent are not important, and most things which are important are not urgent.

Dwight D. Eisenhower

This section addresses aspects of the findings in this paper by providing insights in to the challenges we face, offering some suggestions for improvement, and informs the Future S&T Investment Roadmap 2035-2050. The Future S&T Investment Roadmap speaks to both the immediate and long-term investments required to provide the necessary foundation and capabilities to address the findings and realize the Future Intelligence CONOPS 2035-2050.

In discussing challenges, it’s useful to reflect on one’s experience and history. The following two exemplars cover the past twenty years. The point – that some things don’t change – at least not easily.

It was 1999, when I first drafted and briefed several of the Intelligence Community CIOs on “Concept 2015.” Concept 2015 (Appendix B: CONCEPT 2015) provided an approach towards realizing a more fully integrated intelligence enterprise (ala IC ITE). It enabled proactive identification and profiling of bad actors (ala insider threat). Moreover, it called for a paradigm change in how the IC operated – by strongly urging a paradigm shift in moving from primary use of top-secret sensitive compartmented information to an 85% solution in seconds using totally open source information. Without exception, the briefing was kindly greeted by the several agency CIO’s briefed with the comment “good idea,” but quickly followed by “good luck.” Concept 2015 was never materially enacted. Why do I raise this exemplar? Because these events took place just prior to 9-11-2001, the day the Twin Towers fell in New York, City. Twenty-years have gone by, with little change. Albeit efforts like IC ITE, Insider Threat and OSINT have been advanced, they fell far short of how the IC needs to operate and limits effective intelligence. Secondly, I raise the Concept 2015 put forth, as it faced the same challenges that we still have today – they are cultural and structural. In 1999, the member of the IC, to include each independent CIO, had no compelling need nor desire to upset the boundaries or controls of their individual “titanium cylinders of sub-excellence.” The system rewarded protection of their cylinder, not advancement of the whole.

The next example occurred little over a decade later in 2011. At the time, in discussions with the Principle Deputy Director of National Intelligence (PDDNI), the question about the IC’s ability to implement the concept of IC ITE was raised. The PDDNI had asked what the biggest hurdles / impediments where to advancing the IC ITE concept. I stated that the hurdles were policy and authority. First policy, in that there was no national intelligence policy that could be enforced to drive the IC elements to implement IC ITE. Second, budgetary as until the laws for use of funding were addressed, the DNI nor the IC elements could be compelled to implement IC ITE. I stated that unless those issues where addressed, any efforts to drive the IC to a common framework would be a “mother may I” approach. And, given the prior experience, I stated that success was unlikely without budget authority and policy changes. Any chance of success would be highly dependent on each agency agreeing to fully collaborate, work to the benefit of the enterprise, and do so at potential disadvantage or impact to their own agency. Or, if ODNI leadership were to provide enough incentives or pressure to gain their support. IC ITE was held together for the next several years via the personal will of the PDDNI via meetings and pressure put on the deputies of each agency. It was only a matter of time before this effort, personality-based, would succumb to the culture. That occurred pretty quickly upon change in administration.

We are now nearly a decade later in the future, but these same policy and budgetary hurdles remain, along with others. Another key policy that requires change to enable optimal future intelligence operations 2035-2050 are those that deal with use of open source. The policy and laws significantly constrain the IC from ease in use and or sharing of open source information. Once an “intelligence” element touches open source data, policy restricts its collection, storage, use, sharing, etc.

Enabling a future intelligence concept of operations requires us to undertake several major policy changes. They are not impossible, but require breaking some significant glass and upending some long cultural norms. However, if we fail to do so, we must remind ourselves, that our adversaries have no such restrictions. Our peer adversaries direct their government, private sector, academic institutions to fully integrate and optimize. We must figure out a way to incentivize such integration.

The Future Intelligence CONOPS 2035-2050, projects that intelligence will move from being a key enabler, to being at the front end of the spear in driving proactive influence operations in the competition phase. Regardless of who is lead, operations in the cognitive domain are going to require a new construct that doesn't exist today. Such operations will require an integrated whole of government cross-functional cell of intelligence, information operations, cyber, policy, technology (signal or CIO being part of that), etc. The operation's will likely be further enabled by reach-back to an extensive network of sub-ecosystems that provide expertise in economics, criminal networks, financial, trade, cultural profiling etc.

The current military intelligence foundation data is far from sufficient in conducting operations in the cognitive domain. As suggested in the latter paragraph, conducting operations in the competition phase requires pristine insights and in-depth knowledge that currently exists in pockets and remains incomplete.

Details are required from multiple facets and information domains that go well beyond today's traditional military intelligence foundation data. New partnerships and coalitions will be required with industry, academia, private sector, and other nations/allies. Intelligence (and general force) cannot live on current conscription efforts and must look at other means to rapidly augment intelligence or other functions (e.g., cyber, logistics, medical, etc.) with SMEs from across varied disciplines. Such expertise in social, political, economic, IoT, technology, etc. is required to enable proactive influence and other operations in the competition phase. In other words, the ability to profile a region, a city, country to depth that allows one to understand the totality of the networks (human, physical, technical and virtual), the interconnections, the key players, and be able to assess the flows, intersections and critical nodes in the flow of information relevant to achieve desired actions and objectives. Conducting successful operations, missions and intelligence require several major cultural, structural changes and paradigm shifts in what we view as intelligence and how and when it can be used, shared, applied, etc.

There are many individual efforts underway to enable the future operating concept. The good news is that there are many elements applying expertise to the challenges of operating in the cognitive domain, with tremendous passion, and dedication to mission. However, I find that the left-hand rarely knows what the right-hand is doing, that there is no forum or place from which to consistently gain insights on current efforts, nor is an overall strategy readily apparent. As such a hundred strategies bloom. Many strategies stretch us in multiple directions, and impede optimizing ways and means to a common end. As such, I offer the following suggestions and future investment roadmap to advance development of the necessary foundation and capabilities while addressing key cultural and structural issues in order to enable proactive influence operations and predicative analysis in the cognitive domain.

A New Factory Floor – Overhauling and Retooling Our National Security Apparatus

Today's DoD and IC were created out of the National Security Act of 1947. For these institutions to remain relevant, requires a total overhaul of 1947 functional structure. The core functions they were built to perform were I&W and preparation for war. The shifts in the access, availability and ubiquitous volumes of technology and information have changed the operating paradigm towards those nations, groups or individuals which can more quickly leverage such access to advance their goals and objectives – whether they be an ideology or power projection. It's time we overhauled our production lines, retool our factory floor, or even build a new factory.

Paradigm shifts are essential to ensuring abilities to operate and succeed in the competition phase. To advance desired outcome in the competition phase / cognitive domain, an immediate rebalance of investments is required. The investments are required to ensure intelligence is adequately positioned to support, enable and drive proactive efforts in the competition phase, and to begin developing predictive analytic capabilities as the norm. The cultural and structural challenges in moving the current bureaucracy and cultures are likely to require real consideration by fitting out new factory floors while we guide the older constructs to end of their life cycle. The initial findings suggest it is imperative for our nation to move from a current perpetual state of reaction to nation states as Russia and China, and move to a proactive and predictive capability to drive reaction to our desired outcome.

Achieving such a capability and expertise requires policy, infrastructure, structural, authority and other changes. It requires an immediate rebalance of kinetic investments to begin building the foundation for the cognitive domain. **It is critical to understand that “any” investment in advancing warfare in the cognitive domain has a multifold benefit in the traditional kinetic (conflict) phase and post-conflict phase.** The foundational intelligence data required to operate in the cognitive domain, if developed properly will by default provide a pristine level of detail necessary to effect kinetic actions and outcomes to our favor. And, just as importantly, such a foundation also provides the value-added insights necessary to address post conflict actions necessary to avoid use/or extract US forces enabling a sustained peace.

We've had a number of security shortfalls in our history. Perhaps we should take a broader lesson from them, and understand one reason they occurred is we continue to use a 20th century set of industrial based processes, capabilities and tradecraft rather than a 21st century information based, technology enabled, approach. Mr. Dan Gallington USNews & World Report article on May 5, 2014 captured a good summary of these mistakes in an article titled “How the U.S. Is Its Own Worst Enemy - The U.S. has a tendency to forget some of its biggest security mistakes.”

<https://www.usnews.com/opinion/blogs/world-report/2014/05/14/us-security-strategy-fails-to-account-for-past-mistakes> .

Whether you agree or disagree with these as being mistakes, we need to put ideas on the table and start fixing a 50yr old plus foundation. Our foundation has cracked, shifted and in some cases completely buckled. It's time to wake-up, before we wake-up to yet another unnecessary surprise. Given the democratization of technology, which ill-willed people and groups do access, the next surprise could be catastrophic. So having an open and frank discussion of ideas now is a relatively cheap, logical, and at worst can result in hurt egos or a papercut. We need to drive informed discussion and solutions *before* another mistake. As our nation is no longer a sanctuary, the next mistake may not be recoverable.

To ensure the relevancy of our intelligence capabilities, it's time to truly shakeup the IC. Leaders must drive change in culture, function, organizations and oversight. A few out of the box considerations include splitting CIA, DIA and integrating all-source, human intelligence. Integrating S&T elements into a few vs 17 to optimize focus on most critical. More so, consider integrating NGA with the CIA, DIA all-source, as it's already close. No doubt, some elements of NSA would also be folded in, leaving the cyber elements to fold into another form. Similarly, elements of the FBI, like the national security division should also be integrated into this mix. But out of this integration, create a truly open source only competitor(s). A competitor with no access to national security systems or assets, focused on information/knowledge and decision enabling. Why? Every soldier to policy maker should be able to ask a question and get a like response in seconds - 85+% solution, in battle or in hearings. Then let that group compete against the all-knowing IC elements that retain access to the most sensitive sources and methods. Also, let that open source element inform the IC part, with accesses to special capabilities, to understand the real value added by our national assets. If we stay in our boxes, they will move, but not by choice. True tradecraft and organization reform must leverage our recent advances in integration.

Intelligence Operations in 2035 cannot be optimized with the current IC construct or framework. The IC has realized some advances in efforts to optimize and integrate our intelligence elements, and there may be a continued need for certain

domain specific tradecraft and expertise. However, such expertise is best leveraged in cross-functional teams that integrate and optimize information from across multiple intelligence disciplines / domains.

Continuation of the 1947 industrial age paradigm that separates our IC elements into what I endearingly call “titanium cylinders of sub-excellence” pushes each of these stovepipes to compete for the same limited set of National and Military Intelligence Program dollars (NIP, MIP) – rather than competing in efforts to enable and optimize integration and production of the best most timely intelligence. Measurement and Signatures Intelligence (MASINT) is a perfect example of an intelligence domain that offers significant benefits, remains wedded to decades old platforms, and is likely the least understood. MASINT is highly scientific and technical, and as such suffers from another problem – MASINT places many senior intelligence officers and generals in an uncomfortable position. Why? Because it requires understanding this highly technical-based discipline. Historically, it is much easier to avoid dealing with this discipline rather than being educated and informed. In simple terms – culturally, it’s easier to avoid the subject than look inept and be embarrassed by not being able to explain or understand the subject.

For the IC, it's time we put the 1950's industrial design on the wall, and build the factory or factories we need for our future. The same is true for much of our national security and defense enterprises. Paradigm shifts are essential to ensuring abilities to operate and succeed in the competition phase.

Refining our Risk & Reward System

A key enabler and critical starting point is an overhaul of our risk, reward and incentive system. To realize the Future Intelligence CONOPS 2035-2050 requires a significant cultural change. We need enable new behaviors, outcomes and true accountability.

Leadership consists of nothing but taking responsibility for everything that goes wrong and giving your subordinates credit for everything that goes well.

Dwight D. Eisenhower

To succeed we must fix the culture. Army Futures Command has a great opportunity to start a new factory floor, but also start a new culture. If we're serious about real acquisition and cultural reform, then we must address the root cause. This comes in the form of an easy acronym – RIP.

RIP: Reward & Reallocation; Incentives; Performance & Protection.

R = Reward system & Reallocation. The key is to address the risk and reward system. For over sixty-years, government (IC, DoD, and Federal) has rewarded control vice enabling, status quo vice risk. The reward system is geared towards control of money, people, program, information and power - not outcome. For those with set funds, reward is based on maintaining or growing those funds, not necessarily timely production nor finding efficiencies or savings. The whole oversight system reinforces the current broken reward system. Oversight and policy actually penalizes lack of spending appropriated dollars, even if it's wasteful.

Reallocation. In our current system, if we kill a program, usually those in the program become (metaphorically) a leper colony. Wow, they just killed so and so's programs, boy they must either be useless or lack the skills needed. Hence, we've found over the years that it is easier to become very passive aggressive, rather than become a leper colony. The challenge is our inherent inability to quickly, efficiently and effectively reallocate talent to other high priority programs, projects, or retraining programs to advantage other priorities. The failure to reallocate results another version of the "Charleston Heston affect" (Program managers will hang on to their program until it's pried from their cold dead hands).

I = Incentives. We must incentivize our people to take appropriate risk, identify ills, and fail fast while reinforcing the importance of lessons learned.

P = Performance and Protection. Performance for real outcomes, and protecting those who identify failed programs, take risk and managers who actually manage their people to success. If we do not fix these cultural ills, all will be for not, and acquisition reform will eat this strategy for lunch. Avoiding the cultural war, will avoid the real challenges in acquisition reform, and those who fail to do so will ... of course RIP!

Remaking the Conscription System & Talent Management – Moving to Whole of Government (coalition/ nation as applicable)

I do not believe our democracy can survive long-term if we try to rely on only the 1%. Society is already becoming more and more detached from the few who serve. The article found via this link provides one indicator of where we are headed. <https://www.stripes.com/news/pentagon-military-civilian-disconnect-could-endanger-all-volunteer-force-1.507427>

A 30% mandatory conscription into armed forces, with movement towards 40-100% mandatory conscription into US government service for 2-3 years is not an unreasonable way to advance our nation's security. But a different form of conscription than our current processes is required. And the approaches need to be piloted first, then slowly expanded.

Why? Because our current system is beginning to show it can't keep up with the demand. And, the current system is creating, by default, another "class" of Americans who serve, but to whom the general citizen can barely relate. Platitudes of praise, parades, discounts, and flashes of videos with parent reuniting sort of exemplify the slow path to detachment that is now underway between those who serve (the 1%) and the rest of our public. A fairly recent gallop poll highlights an aspect of this challenge.

<https://news.gallup.com/poll/236420/record-low-extremely-proud-americans.aspx>

By reforming our conscription and talent management systems, strengthens the bonds between our citizens and our military. If done right, we will create an ecosystem unparalleled in support of national security, freedom, democracy and that once again realizes a true melting pot by enabling, innovating and building trust, freedom and friendship across all races, religions and cultures - in advance of our national security. A dream, I think not. But again we must think big, start small, multiple pilots, educate, communicate and scale.

Future conscription should consider a model whereby our citizens do not have to serve solely in the military, but expanding the service to other key economic, policy, and national security areas. Growing partnerships with the private sector and academia builds trust, understanding and advances benefits for all participants. This is not an unreasonable goal. However, it is likely not a politically obtainable goal for the near-term. So, let's get started. Let's do some pilots. And let's educate ourselves, our overseers and public on the overall benefits by providing positive proof. Hmmm. A novel idea.

It is not a struggle merely of economic theories, or forms of government or of military power. At issue is the true nature of man. Either man is the creature whom the psalmist described as a little lower than the angels ... or man is a soulless, animated machine to be enslaved, used and consumed by the state for its own glorification. It is, therefore, a struggle which goes to the roots of the human spirit, and its shadow falls across the long sweep of man's destiny.

Dwight D. Eisenhower

Across our IC we do not, and cannot obtain, the level of expertise required in all areas, all disciplines required to advance in the cognitive domain and operation in the gray zone. To address critical shortfalls in expertise, we must begin to build new ecosystems that create trusted networks of expertise across social, economic, cultural, biological, anthropological, financial, technical, etc. disciplines. Our national security fabric inextricably bounds private sector, academia, government within one umbrella, but we continue to act as if these are wholly disconnected piece parts and ignore the critical touch points within this fabric. Unless we strengthen those touch points, the fabric will remain relatively easy to rip. If we begin to take a more holistic approach, ala whole of government, whole of nation approach, we can significantly strengthen the fabric while concurrently providing value to all participants. Micro examples of this occur today with the private sector, academia and government via paid internships. Other countries are building new recruitment structures where they tap into such expertise, but not necessarily placing them in military uniforms.

Future Operating Environment & the Character of Warfare 2035-2050

TRADOC has published multiple documents, papers and briefings that put forth views on the future operating environment, character of war, and Multi-Domain Operations (MDO) that speak to the timeframe 2030-2050. The Chief of Staff US Army' Futures Study Group (SSG) also put forth their views of the future in "The Character of Warfare 2030-2050." Both offer varied insights, views and comments as to what the future holds in warfare. I could repeat much of what they've laid out here, but that's not the purpose of this paper. Suffice it to say this paper leverages those foundational inputs, but challenges their focus on kinetic capabilities.

The SSG looked at the relevance and state of technology in 2035-2050 and arrived at the conclusion "...Game-changing technology will be slower to materialize than promised...There is a nearly even chance that the rate of technological invention will slow^{viii}." Given today's focus on technology competition, projections of the use of AI, etc. one would think that is somewhat of a startling projection. However, as this paper addresses, if we stay the current course, remain predominately reactive, do not adjust our production lines or overhaul our factory floor, that the SSG's finding on game-changing technology will likely be correct – that is for the US only. We will remain significantly disadvantaged in adopting, using and deploying new technologies given the cultural and structural challenges we have, our industrial age acquisition processes and policy, the lack of an integrated enterprise approach to portfolio management. However, as adversaries dictate, direct and drive more fully integrated portfolios of capabilities that leverage each other, understand and use of a whole of nation approach – it is likely they will surpass us.

This paper challenges a predominate focus on kinetic capabilities, recommends a rebalance of investments and efforts to enable and conduct operations in the cognitive domain, and believes that the future operating environment, MDO, etc. will be more heavily directed, influenced and actioned in the cognitive domain. Neither TRADOC nor the SSG fully ignore the cognitive domain. One example, the SSG report states "While the risk of military dispute between regional powers that escalates into a larger conflict will continue to decline, the number of intrastate conflicts and gray-zone competitions will rise.^{ix}" However, this paper projects that unless we adjust our future CONOPS and S&T Investments to account for that a paradigm shift of operating in the cognitive domain, our nation and its intelligence operations will once again awaken to a mistake.

Future Military Intelligence CONOPS 2035-2050

Intelligence in 2035 will be based on a wholly new paradigm of primarily using readily available open source information, vice focusing primarily on highly classified sources. To achieve this, the normal understanding of foundational military intelligence will also undergo a significant overhaul. Today, foundational intelligence data primarily deals with orders of battle, infrastructure, and potential military targets. As we operate in 2035, we'll need to operate in the cognitive domain. Intelligence operations will provide an in-depth understanding, tracking and assessment of every region of the earth, its people, and their cultural dynamics that include every aspect of the culture and its ebbs and flows. The analysts, collectors, operators, etc. will leverage a new type of foundation data that is pristine by comparison to today's military intelligence foundation data. More astounding, the greater majority of the data and information will be primarily open source. The intelligence apparatus will have realized that it's not just big data, but the right data. The right data being that information relevant to solving specific functional needs that is curated, validated and veracity assessed. The data and information will be partially collected, other purchased, accessed via the internet, accessed via off grid sub-nets, or captured via live streaming from unclassified and open sources. The uniqueness of the information and data will come from its source, the validity of the information, the veracity and volume and via continued and regular updates and assessments of its quality, validity and to ensure its not been altered purposefully or via others means.

The information and data will provide the basis to profile a region, country, city, individual or group (physical or virtual) based on understanding, mapping and then building a pristine profile that captures normal, action, etc. which can then be used to profile and set trip wires for specific activity. The intelligence operator will drive planning in concert with a new and unique set of partners from across the government, allies, and other coalition partners – to include tapping into new trusted ecosystems and networks that cut across the private sector and academia. The ecosystems will not consist solely of US private sector, government or academia – these networks will span the globe touching the right subject matter experts to gain, assess and plan for proactive influence operations, provide predictive intelligence analysis, or inform target specific kinetic actions from an individual to broader groups.

This new paradigm shift will have occurred starting around 2020, as the IC realizes that they can no longer keep up with the volume and masses of data, no longer needs to, but can tap into and build integrated profiling of individuals, regions, cities, or country's using basic analytic methodologies and applying basic machine learning (ML) and advanced processing. The intelligence analysts will have realized that while the data may be never ending, that there are and will be only so many data and information sources at any given time. All of this is predicated however by the right questions being asked of the AI/ML also. Data without proper analysis is worthless. Determining which are the best, most valuable, and pertinent will depend on the type of predictive analysis, influence, operation, or kinetic action and desired outcome. Future intelligence operations will not focus on the big data issues, as big data is really an annoying distraction. Future intelligence operations will continually assess, vet and validate the primary data / information sources required to support overall national security objectives and missions. Once initially vetted and validated, regular review and assessment of the sources ensure freedom of corruption. What will these new foundational intelligence sources tell us that's different from today?

The military intelligence operator and analyst will integrate even further, and actually lead most major military operations. They will integrate into whole of nation, whole of government, and broader allied / coalition networks as mission requires – but bring the unique insights, tools, and capabilities to detail the social, political, economic, biological, chemical, nuclear, criminal, etc. networks, the players and their regular actions and activities in a region, city, country or conglomerate that covers several areas on the earth. Whether criminal, regional groups, political etc., the amount of data and types readily available either on individuals or on groups will be more than sufficient to profile, assess and begin to layout trip wires while supporting predictive analysis.

The latter capabilities and efforts began to take hold in 2020. True optimal fruition begins at the start of 2035. This is because the cultural resistance, paradigm shift from using primarily classified sources to majority unclassified sources, development of necessary methodologies that aid in linking the varied networks (e.g., criminal, social, political, economic, etc.) and establishing a persistent cataloging and vetting of data sources will be achieved for only a few major cities and regions by 2035. However, the foundation will have been set and allow for more rapid scaling of capability in the years 2035-2050.

The ability to provide a Common Operating Picture (COP) from private to president, simultaneously, in real time and the level of insight provided, along with the ability to forecast and predict varied activities, etc. will drive a thirst for covering the globe in such foundational information. With the aid of distributed ledger and other technologies the same information will be parsed out to who needs it. We will shared it with our NATO, coalition or other allies – to include proxies or

insurgent elements – at the speed of light and in a more secure way than the classified networks of 2020. Use of IoT and other technologies will provide redundant, resilient and survivable networks in peace and threat environments, while also avoiding vulnerabilities that allow access for attackers.

The inability to deploy mass formations from US shores to overseas locations was realized around 2020, and more fully accepted by 2030. The rapid fielding of new commercial space sensors, increase in UAS/UAV sensors for use in varied commercial industries, continued expansion of social media and the massive expansion of IoT devices led to realization that keeping any military action covert, hidden, or unobserved was becoming near impossible. In certain remote areas the geography or other natural features would help to obscure movement or activity, but even then the new sensors, 5G capabilities and increased natural integration of varied data and information sets – it was becoming more and more difficult to hide movement. The days of shipping large formations, supplies, etc. to another region, building up the foundation for a major kinetic assault or maneuver, were slipping by – but would likely never be allowed again in any contested environment. Achieving the element of surprise required a new level of intelligence, awareness of the local region and infrastructure, and the ability to operating and hiding in plain sight. The ubiquitous nature of sensors, information and technology by 2035 will increase the challenges of operating without detection. The use of large formations began to die off in 2020.

The advances and fielding of new capabilities by Army Futures Command in early 2025-2030 began the restructuring of Army operational formations to much smaller, mobile, agile and effective units. The major impetus for change came not only from the threats detailed by intelligence, but from how intelligence was more fully integrated not as just a supporting function, but as a primary partner in mission command of any operation. The old military mindset that those who pulled the triggers on kinetic events drove the mission had flipped. The complexity of the missions, need to integrated multi-domain capabilities, and requirement for everything from discrete influence operations in the cognitive domain to surgically applying kinetic effects, required a new breed of commander.

Another advance in technical capability, that altered intelligence operations, came in the form of new power sources that provide the means to build totally independent networks, separate from the grid. The use of solar power was a secondary and enabler of powerful flywheel technology that allowed our posts, camps, stations to begin moving completely off-grid. A small solar source was used to start up the flywheel, which in turn provided tremendous regular or surge power as required for large to small organizations or locations. The technology by 2040 was advanced, leading to its miniaturization for use in tactical environments, for vehicles, etc. In parallel with the fielding of 5G, and due to continued concerns about internet security, more and more of the populace was moving off-grid. People were moving to their own secured extranets. These extranets were very tightly controlled in access and membership. The beauty of this was that the internet continued to excel, but new versions of biometric security controls drove a commercial boom in creation of extranets – for banking, social media, and about 10-years into the rage, the DoD. The mixture of new power and network technology enabled US DoD and its intelligence enterprise to disperse, move off grid, and leverage more fully not only the internet, but the billions of IoT sensors and devices fielded over 2020-2040. In this mixture, the intelligence community along with several executive branch departments and allied governments proactively dispersed, embedded, etc. millions of our own unique IoT sensors. These efforts enabled very resilient communications in friendly or denied environments, using an integrated and layered set of networks, sub-nets; IoT based networks; Wi-Fi networks, etc.

The intelligence operators during 2023-2030 began to develop very in-depth foundation data necessary to set profiles and trip wires for support of tactical and strategic operations in the cognitive domain. During late 2020's into late 2030's we also were working with our allies in leveraging the overall growth / deployment of IoT sensors (i.e., commercial, government, private sector, academia etc.) in establishing a robust foundation for the cognitive domain. The shared base ideology for free and democratic governments advanced an inherently natural partnership. By 2040, we'd developed profiles for the most urgent set of individuals, regions, cities etc.

The intelligence operators efforts, began to slowly impact the old cultural concepts of having the “trigger puller” (e.g. tank, fighter, destroyer, etc.) as being the default mission commander. The shift to a blend of trigger pullers and intelligence operators was becoming more of the norm by late 2035. Those who resisted this shift knew it was only a matter of time. The commander of 2035, no matter the military service, required an in-depth knowledge and expertise in intelligence operations, strategy and planning in the cognitive domain, and an ability to lead a diverse whole of government team. Expertise in the kinetic realm didn't disappear, it was a relevant as always, but more typically involved supporting roles vice the primary role and driver. The inevitable movement to enhanced operations in the cognitive domain shifted intelligence operators from a supporting to a directing role. The services realized more and more, the need for a hybrid set of leaders. A new mold for mission command required leaders steeped in the future intelligence operating paradigm, backgrounds in data or social science, cultural anthropology or knowledge management, and ability to operate, integrate and collaborate across a whole of government fabric. In simple terms, the most effective future intelligence operator will have a mix of a business,

the arts (e.g., music), science and/or social science expertise. The value of the arts comes from the ability to deal with the abstract and improvising.

Given increased ability to predict activity and determine the best ways and means to influence towards a desired objective or outcome, intelligence and operations in 2030 were being driven by regional strategies to support strategic influence operations. The integration of regional strategies was still a challenge, but the culture was getting there. But, this new truly strategic approach purposefully minimized kinetic efforts and advanced “whole of government” or “whole of nation” efforts. The objectives and outcomes in driving proactive influence were understood to be a longer cognitive game of chess, vice a short game of kinetic checkers. But by 2035, these strategies were accepted and supported not only by Legislative branch overseers, but were becoming part of a strategic approach to national security that was maintained between political parties as the White House switched hands.

In 2040, the overhaul of several elements of the Executive Branch that began in 2025 was still in motion. However, the continued success in achieving desired outcomes and impacts from overhauling the IC and several major element of DoD was whittling away the last vestiges of passive aggressive resistance. The blending of military, national and regional intelligence was a no brainer, given the move in using predominately open source information to optimize our OODA loop. At the same time, the integration of national and tactical intelligence significantly advanced proactive influence operations, and conducting predicative analysis. The playing field was one and the same. Strategic objectives were actually driving well-planned tactical operations. The new foundation information enhanced operations in the cognitive domain by providing real time feedback on the local populace reaction and engagement, while providing insights into whom the key

THE THREAT that authoritarian political warfare poses is therefore real and persistent, and strengthening U.S. defenses is imperative. Hardening electoral systems and cyber defenses, shining greater light on Russian and Chinese influence activities, cracking down on the dissemination of disinformation, devoting additional intelligence resources to detecting malign activities, and strengthening cooperation with allies and partners facing similar challenges are critical to limiting the damage authoritarian political warfare causes. For several reasons, however, a purely defensive posture is neither sufficient nor desirable.

<https://nationalinterest.org/feature/how-wage-political-warfare-38802>

players would be to interact with, influence, etc. Intelligence operators were taking the leading role in well-planned and choreographed operations. The playing field was preloaded by proactive engagement and influence of the key networks and players so as to affect not only desired tactical action, but the keep the longer-term influence operation on track.

The distinction between military intelligence and national intelligence became completely gray, with the rare exception of specific kinetic action. Proactive influence operations used an integrated set of tools to proactively achieve desired impacts/outcome. The unique data sets and information supplied by intelligence in 2035 provided the most pristine Common Operating Picture (COP) in real time so that each echelon could tailor the depth and detail of the information and COP to their specific mission set. In other words, if a platoon is going in to conduct a special operation or support a humanitarian relief effort, they will be able to tailor the regional data inputs and information to provide them an ability to replay the regional profile against their specific mission. They can understand how to hide within the noise, circumvent and avoid setting off local trip wires by aligning their actions to normalcy in the profile, and intelligence support can then focus not on the mass of data, but the few elements or data points that could cause potential disruption for the mission at hand.

The intelligence CONOPS of 2035 enables the masses to operate using open sources to optimize their specific mission OODA loop, while the use of national or unique classified intelligence capabilities focused on detecting micro indicators to keep such operations invisible to the local populations. The ability to provide such pristine insights and profiles required a paradigm shift in the use of open source information, but also required a paradigm shift in how we capture, produce and maintain such foundational data. These shifts were hard, and involved a complete overhaul of the big 6 IC agencies which began in 2020-2025, and finally began settling down in 2040.

The incredible shift in capability, and providing it at all echelons, significantly impacted the size of the Tactical Operations Center (TOC) during kinetic operations, and fused tactical and strategic operations for regional efforts. The ability to

leverage the profiling and information via AI/ML and other information technologies, changed the paradigm of intelligence being primarily a supporting role.

The foundational data this future intelligence CONOPS required a “whole of nation” effort, across multiple networks of subject matter experts (SMEs), and multiple non-traditional intelligence domains. In other words, future intelligence operations will rely on production of foundation data from non-traditional sources that include US financial, bio, chemical, law enforcement, educational, social, political, military etc. ecosystems and networks. Overcoming cultural, political and organizational resistance to use of intelligence in this manner occurred after several parallel pilots where the outcomes spoke for themselves. Given the predictive analysis, new skill sets and ability to effect proactive influence from the tactical to strategic level, from POTUS to policy makers and operators, they saw that this new operating paradigm from intelligence provided the nuances and deltas that afforded the 1% to 15% decision advantage over our peers and adversaries.

Getting to such effectiveness was a major effort, as it took smashing a number of “titanium cylinders off sub-excellence” and driving them into truly integrated and collaborative elements. We began operating as a true whole of government enterprise, vice competing enterprises by service or organization. The new breed of intelligence professionals realized that they must focus on the understanding of profiles, varied dynamics of multiple human/physical/virtual networks, the interpersonal dynamics, and flows of information to articulate, educate, plan and effect operations that influence, exploit or impede either the actions of our designated target to change or react.

Intelligence in 2040 no longer made a distinction between national or military. Intelligence morphed from providing general assessments and overviews of near-term and distinct tactical actions, order of battle, and regional summary to blended intelligence. Intelligence began focusing on specific multi-dimensional assessments, with in-depth insights into the key networks, players, that afforded decision makers (military, political) multiple options, increased understanding of the risks, and likelihood of success in effecting desired impact desired outcomes of an individual, group or nation state. By 2040, we had achieved the ability to conduct predicative analysis consistently. In the majority of instances, that enabled proactive influence operations across multiple regions, cities, or at the individual level. However, we realized to sustain this advantage required diligence, continued refinement, and avoiding historical tendency in becoming complacent with the current production line and factory floor yet once again. In other words, the new IC learned how to move towards continual refinement and improvement.

While our adversaries began to understand they were being impacted in many ways (e.g., socially, politically, military action), they did not yet comprehend our new means, methods or use of information and technology to out maneuver them in the cognitive domain. They realized this the few times kinetic actions were employed with devastating effects.

Intelligence operations in 2040 were now providing exemplar outcomes that clearly demonstrated the ability to leverage predictive analysis, new foundational data, and new more fully integrated whole of government constructs to proactively drive adversaries and opponents to desired outcomes. For the few instances where that approach did not work, the pristine foundational intelligence by region, city, individual allowed for much more specific targeting – from an array of tools, not just kinetic. Given realities of the human condition, specific tactical kinetic actions were still relevant and useful.

During the earlier years (2020-2035), the relevancy of intelligence and our IC or combat agencies had been called into question. No longer could we sit by and pretend we had the premier capabilities, sources, or methods. The world had moved under our feet, and what was high cost with few participants, was now low cost with millions involved. What happened?

With the advent of multiple launches of small satellites, enormous expansion of IoT sensors and devices, the advent of additional ML/AI into social media and creation of small to large, integrated to distinct, informal networks of “self” anointed analysts. With the plethora of sensors and information, what had started as part time hobby to watch key events in countries like Iran, Syria, etc. had morphed into groups of patriots, non-governmental, allied, and cross-national humanitarian elements. These groups realized they could weigh into the world’s national security arena – by highlighting key events, key activities, and support tracking of anything from illicit drug shipments, proliferation to human trafficking. The dynamics of the intelligence world was upended by this expanded use of open sources. Sources were open to the public or accessed via a small fee. The masses began to crowd source analysis – and some of their groups were exceptional.

To remain relevant, the national security apparatus began a major overhaul starting in 2020. It was leveraging the broader open source foundation to support cognitive warfare, proactive influence and predicative analysis. The IC and DoD morphed without realizing the extent of change within. The bow wave of retirements opened up influx of new breed of

intelligence professionals already steeped in operating in this new paradigm. The cultural change therefore was not as difficult as some thought.

While initially, this mass of anointed student, amateur, and other analysts started out as a perceived threat to national security – this new construct was nurtured along by some of the forward thinking intelligence operators a capability to selectively “crowd source” some of the persistent and most human intensive monitoring and assessment problems. The results were amazingly beneficial – as the amateur to expert analysts inputs were assessed, categorized and then feed into open source feeds for our profiles of regions, cities or individuals. Without trying, we had enabled a whole of nation and beyond network of citizens who sought to advance the human condition – and we were able to begin tapping into that source of unique analysis. Of course, many of these self-formed groups didn’t want anything to do with government oversight or intelligence, they saw themselves as competitors for the truth. Nonetheless, the value added was exceptional. After getting past cultural hurdles and hurt feelings of the “experts,” the intelligence operators began to realize they could now outsource / crowdsource much of the “mundane” and via the competition between peer groups of these self-formed networks – realize a level of tradecraft, that while not perfect, was valuable.

The intelligence operators reached out to select groups, much like we had done in the early 1980’s to the white hat hacker communities, and began to build trusted but open source ecosystems. These new networks of analysts and SMEs from across the private sector, academia, former intelligence analysts, etc. were used to assess and advance the best sources and efforts from the broader networks. And, for specific problem sets, rather than react in a crises – our intelligence operators were able to quickly engage, collaborate and task the trusted networks – which also included a means to reward or pay those SMEs for their time. A truly win – win situation. By 2035, the use of crowd sourcing analysis, and tasking trusted ecosystems/networks of SMEs had become the norm. With this mass of new self-anointed analysts and use of open source information sets – the IC and DoD were further pushed to accept the paradigm change in efforts and realized they either accepted their efforts, and stayed ahead of the curve by leveraging and leading, or becoming mostly irrelevant. With the multitude of sensors, information, etc., the IC and DoD intelligence operators began to add value on top of the 85-90% solutions they were provided in minutes or seconds, by integrating the truly “unique” intelligence sources and methods into their final products.

By 2035, all military and intelligence operators learned that their operations in the cognitive or kinetic domain required extensive planning and preparation, for the norm had become to conduct operations while hiding in plain-site. This new intelligence foundation and ability to affect specific actions to the individual caused our adversaries to pause and reconsider actions detrimental to the US or policy. As the level and understanding of the varied physical, social, criminal, economic, etc. networks and individuals continues to expand past 2035, our intelligence operations will use that foundation for even more specific action. The intelligence operator were quickly identifying the most critical individual(s), determining options for action against them or the networks they are tied to, and providing decision makers options from the removal of that person from existence or several ways to perturb their existence such that they will think twice before taking any negative actions. This was quite the change from 2019, when many of these actors stole, conduct cyber operations, or undertook criminal efforts with little attribution or retribution. Intelligence of 2035 and beyond, with access to levels and quality of information never before realized was targeting, eliminating, mitigating or penalizing such actors immediately and with severe consequences.

There is a caution. Our peer adversaries gained access to much of the same technology and information. Unfortunately, at the outset of this new operating paradigm back in 2020, our adversaries had a significant leg up on us. Hence, the real challenge in the cognitive war was to be able to surpass and sustain such capability.

Because of the paradigm shifts, the number of tactical kinetic actions and threat of regional or peer/near-peer conflict were diminishing. Our adversaries were now reacting to our shift in how we use intelligence, how we were able to integrate and leverage a whole of government/nation approach without resorting to dictatorial powers and subjugation of our citizens. They also realized that this new approach, continued to rely on limited and focused kinetic actions, but that now the US understood and dominated in the main battle space – the cognitive domain. We had finally realized that we were in the middle of a cognitive war that would last a millennium or more.

The next few sections detail both threat scenarios and operational scenarios that could likely play out in 2035 or sooner, using the Future Military Intelligence CONOPS 2035-2050. They are fictional projections.

The following scenarios are fictional, but meant to highlight certain potential vulnerabilities and risks given the state of technology today (2019) and what it portends for 2035-2050 in terms of potential conflict for US forces or our nation. Additionally, there is a scenario of how the Future Intelligence CONOPS 2035-2050 could effect outcomes in the 2040 timeframe. While these are fictional scenarios, the state of technology is such that enabling such scenarios is possible currently.

Bio-Warfare: Realizing Precise Elimination – 23&Xi

An adversary intelligence element was discussing the best way to actually place the US at major risk by creating and developing a means to cause limited to massive catastrophic impacts, but do so with little to no means for attribution. At the same time, devise methods of development for the capability that actually involves the adversary paying for, supporting and advancing it without their knowledge or awareness.

So they began with an assessment of the cultural unique aspects of the US, and what types of areas were of interest to the general population. Given the explosion of genetic/DNA testing, fertility treatments, and new means to biologically determine lineage – and a long history in the US of tracing ancestry lines, one of the foreign analysts devised a schema, methodology and put it forward for the party's senior review. It was immediately adopted, blessed off on by the Adversary politburo, and put into implementation. The government funded and established a DNA / ancestry site that promised insights into your family ancestry, health checks, etc. all for under \$100. The response from across America, and globally, was astounding. The business of “23&Xi” was a booming success.

The intelligence professionals were ecstatic, not only was their plan a success. The program was not only fully funded by the legal commercial business established for this operation, it provided significant additional profits over expectations. The program began a few decades earlier, the timeframe was now early 2038, and the adversary had now achieved an ability to map family lineage, DNA, and capture information that identified groups of citizens by race and other criteria not only in the US but for much of key western powers.

What wasn't so well known, but alluded to in varied intelligence circles, was concern and projection of the adversary using biomedical, DNA, and other means to develop a means to affect, alter or eliminate targets – individually or by race. They had been using such experiments on a subset of their own population, unknowing, for years. They had mostly perfected their means and methods, but they were still had a few bugs to work out.

In 2038, the adversary was fed up with their neighbor, and independent and isolated island nation, that continually refused to unify. Because they had a few bugs to work out in their capabilities, but wanted to resolve this long lasting dispute. They put their plan into motion. They would use their DNA/gene analysis and targeting methods and let loose certain strains of virus that would lay dormant for at least six months. It would be triggered at a time of their choosing.

The adversary nation called for a major meeting of key players – the island nation and leadership, and their politburo. At the meeting, all were served the same foods, drinks, etc., with one exception. The food given to their island nation's leadership contained the unique virus, developed from the 23&Xi data. Of course the meeting achieved little, the adversary left abruptly at the end and stated they would work hard on some counter proposals.

Unfortunately, six months later, the dormant virus began to react. The targeted DNA of the island leadership lead to a multitude of deaths, severe health issues, and affected up to 15% of the rest of the population. The adversary nation stepped forward to provide aid and relief efforts under the auspices of humanitarian efforts. The US, at the time was not able to react as quickly, so they deferred to what they assumed was a legitimate assistance effort. It was a ruse, and with the deployed aid came special force elements that assumed control of several major island defense, policy, legislative and other government organizations. The island nation and the US were caught unaware. At this point, any military or other intervention would mean millions of lives lost on the island nation, or from casualties from direct conflict with the US. Their plan was not only effective, it succeeded stupendously.

They now began to assess their next attack, given no suspicion or even awareness of where the virus came from – given it was not traceable to anything other than normal genetic elements. Their next attack was on US political leadership – Congress and the Executive Branch. Their focus would be disabling, not killing, key leaders. But, their likelihood of success

in removing the US as world-leader or major player, for a decade or more, was now underway. During the timeframe 2020-2030, with their use of extensive AI/ML capabilities, the adversary had created an extensive database of senior US and other global military leaders, as well as major segments of their populations. Although there are a few details to work out to ensure no attribution, their plans are now set. The ability to selectively eliminate an individual, a group, a race or population – or impact it in varied ways was now demonstrated. What would be the adversary's next step?

Post Scenario Comment: Less some think this isn't possible, nor being considered, one only need to look at the latest news headlines and look back into history a few decades ago. One government is supporting efforts to modify DNA. Where are the limits? If a nation has no qualms about subjugating and increasing control over their own population, does one believe they would hesitate action in this arena against other populations, if believed to be in their national interest, and if they thought they could control the level of impact? The horrific experiments on humans in WWII era are a reminder of the reality of such events. Given the recent experiments in one nation, one should not assume any moral or ethical restrictions in advancing their position. The path forward could likely make cyber warfare and security concerns seem like minor offenses. The costs are minimal as compared to advanced weapon systems, and can be applied universally, with the right sets of data. As some nations consider the state as supreme, not the individual, all else is subject to ready sacrifice.

The above scenario is not the sole prerogative of nation states, as there are examples of individuals using gene editing etc. and experimenting on themselves. As such, the lone wolf actors may create major issues with readily available technology. As with technologies such as Crisper, these capabilities are not necessarily confined to a nation state.

Lone-Wolf and Virtual Nation Chaos

The technology scouts were asking the vendor how much it would cost to obtain a subset of data that would allow them to track cell phones in a specific area over a period of several-months. The vendor stated they could provide a simple subscription and that would cost several thousand dollars, but they could then select the areas as desired – and do their research. The vendor did note that specific information on individuals was not included in the data, and actually prohibited from law to obtain/sell. The tech scout asked if the generic cell phone IP address etc. was part of the data purchase, the answer was yes. So, he signed a contract and paid a few thousand dollars, and began to set up his research project.

The tech scout came back to his home base, where there was a mix of US, foreign national citizens – but all with one desire. The desire was to put the US into chaos, so that they could advance and realize their goal – anarchy. Or, a version of anarchy that they thought would undermine the US position with respect to other countries. This group never wanted to see US hegemony again. They obtained funding, from a variety of radical groups that opposed US hegemony. They had set up a simple non-profit to advance certain ideological beliefs in countering “big brother.”

They began their research by drawing data collection circles around the US Capitol, the White House, and Pentagon. They then purchased and used a variety of readily available commercial data sets that included social media, economics, credit card use, real estate data etc. They then plotted, monitored and assessed the data over several months. Slowly but surely, they found the specifics they were looking for. Using the commercial data and cell phone data they were able to track White House and Capitol Hill personnel across the US to varied locations –. They plotted locations where the cell phones went off (e.g., Pentagon) and then other locations not so obvious (including the secret locations). They then began to cross correlate the data and identify specific homes, the persons who lived there, etc. So, even though the cell phone data they purchased did not contain individual data, the other data sets they had allowed them to find, locate and map the daily routines and travels of the SCOTUS, POTUS, NSC/Cabinet members, military and key Congressional leadership.

While the effort was exhausting, it only took seven months with their team of data scientists and experts in varied technology disciplines. They now had their desired data. In parallel, a smaller subset of their group, funded by a nation state via several back channels, began to put their real plan into action. Their target date was the State of the Union address – occurring in less than two months.

This smaller group had also purchased programmable/autonomous UAS drones, and been working on with programming these drones to seek certain cell phone Internet Protocol (IP) addresses. The type of drones they purchased could travel up to 20 miles one-way, with 10lb payload. They’d been experimenting and testing with these materials and coding for several months. They realized a high percentage probability of being able to intercept the IP addresses of a cell phones and deliver their package. Their plan was now ready to set into motion.

On the night of the State of the Union, they waited until the President had finished her speech. It was her inaugural State of the Union speech, having just been elected in 2032. They waited. As the varied members of SCOTUS, Joint Chiefs, senior congressional leaders etc. began to depart the Capitol – they launched their pre-placed drones via signals sent out via LoRa (short for long range), Wi-Fi, and other networks using distributed ledger technologies that would make retracing, extracting or decrypting the signals nearly impossible. The action had begun.

Within the next hour, chaos blanketed the Capitol. Several members of Congress were assassinated, along with three of the Joint Chiefs, several NSC and cabinet officials – the POTUS and VPOTUS survived, only because they had extra armor on their vehicles. Sadly, several secret service agents that were in the motorcade did not.

Their plan was a success, chaos ensued, martial law was declared and the nation was put into panic. Not bad for a few hundred thousand dollars in funding to pay for data to track identify their targets. All of these tools were commercially available. The only really hazardous element was obtaining enough explosive material for placement on the drones, but that was easy enough via the black markets and funneling the materials across a still porous US border, in this case via Canada.

While not all of their targets were successfully affected or eliminated, it did not matter. By the time the US government figured out what, how etc. things occurred, the anarchists would be hailed as heroes by many of their radical constituency. More so, with the ensuring martial law and chaos, they then began to push their 2nd and 3rd order plans – looting, riots, taking down power supplies, etc. The US was crippled, and our adversaries knew it.

Mega City & Virtual Elimination

It was three in the morning when the phone rang in COL Johnson's home. He looked at his alarm clock and realized that the mission was about to begin. They had been planning this mission for the last two-months. He looked at the calendar, realizing that in about six hours, he'd be heading to a party for his parents 50th anniversary, and quickly wondered what it was like to live in Atlanta back in the 1990's, with the internet just getting off the ground, and the majority of Americans still using phones where you dialed the number. He barely remembered 9-11-2001, as he was only five years old, and now he was a 44-year old COL conducting an operation in 2040 – from his home!

COL Paul Johnson, or PJ, was one of the first Army intelligence officer to accept integration into the multi-service intelligence element under the new Space Force created by then President Trump. He was also one of the first to participate in a bold new experiment the DoD and IC undertook in 2025 as they overhauled the IC and DoD Combat Support Agencies, creating a new Open Source Element (OSE). The OSE did away with that annoying term OSINT (or open source intelligence). The term OSINT was created by the IC to fit open source information into their world. Our national security leaders realized we'd tied our own hands by limiting and leveraging the use of timely open source information to support operations.

PJ led and directed part of the laydown for new foundational intelligence for Tripoli in early 2020, and then led similar efforts working on greater Libya. He leveraged a whole of government team that consisted of IC, Treasury, Commerce, State, Energy, several specific DoD cells, with the litany of subject matter experts (SMEs) you would expect as well as others from law enforcement, Interpol. This extend to several allied ecosystems/networks of SMEs They also tapped into their broader private sector and academic ecosystem – bringing in specific regional, country, cultural, political, criminal, etc. experts. During their efforts they mapped the varied networks, identified the key players, dependencies, etc. and in a year they had laid out the profile and key trip wires for key areas of importance from terrorism, to criminal/drugs, human trafficking, political, etc.

PJ's mission focused on eliminating a few individuals who were financing specific efforts to undermine (what had finally become) a legitimate government in Tripoli. The civil war and disarray after the Arab Spring 2003, had lasted for thirty years. In the last several years, stability and prosperity had come to Libya and Tripoli – but some pockets of illicit activity were growing again – with some foreign sponsors from the Middle East (ME) who lost their power base with the political settlements. The illicit efforts were led by Fayed al-Islam.

The threat to stability from Fayed's efforts could upset the political settlement and relative peace of the last decade. The implications for the US included not only losing Libya back to chaos, but also destabilizing several other influence efforts in the Middle East and North Africa that were also nearing settlement. The POTUS decided, based on use of primarily open source data and information sets that direct action would be necessary to resolve the problem before it got out of hand. The mission was to stop Fayed and close down his efforts, but to do so without any direct military action.

In this instance, although the action was not kinetic, at least from a traditional sense, it would be just as effective. Based on PJ's prior work, they knew of several gangs tied Fayed. They also knew that one specific gang was starting to benefit from the newfound stability both economically and by moving becoming part of the legitimate political establishment. Using their profiles of criminal, economic and social networks, PJ's intelligence operators identified Agulia Al-Gathafi (a distant relative of the former dictator Muammar) as their action man. Agulia, while having moved towards legitimacy, still had some nefarious partners. He still had ties to certain militant elements that had not disbanded. Fayed's and Agulia's militias frequently engaged in small skirmishes.

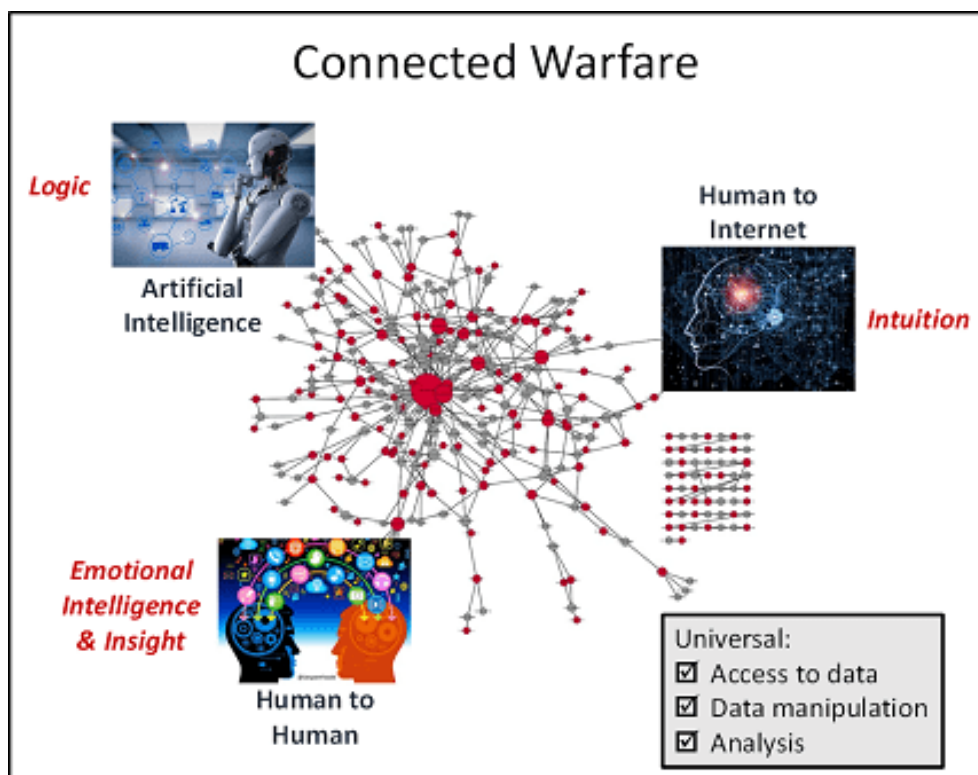
PJ realized it was time for the mission. He went into his den, turned on his electric security barrier and signed into to his AR/VR headset. He joined his team, several other players in this virtual world, as they put into action a pre-coordinated plan. They knew their target Fayed would be at a local disco – that was frequented militant groups. The militant groups had each seized control of several cities during in prior years during the civil unrest. They were competitors in the old days, and they remained competitive today. However, member also frequented the same social spots – in this case a specific disco in Tripoli's southern side. While the rest of Libya had begun to move towards stability, a number of the militias hadn't disbanded. Being part of the militia was all they knew, and while the government was providing new jobs and opportunities, some of them would never change – they liked conflict.

PJ's team, used the new regional and city intelligence foundation to obtain pristine details and insights into the players, their networks (criminal, economic, and social) to determine how best they could achieve their objective – removal of Fayeze. They began by inserting false financial transactions, a social media posts, and using a few local foreign agents on the ground to create the impression that some in the rival militant group had been purposefully undermining their few remaining sources of revenue, while also disrespecting their chief. Tensions were beginning to build, and PJ and his team were continuing to drip gasoline on this fire.

Fayeze had arrived at the disco at his usual time, and was busy engaging with his network on their next scheme. He didn't realize the tension between the rival militants was growing. But he would soon find out. The local time in Tripoli was early am. The disco party was in full swing, the noise loud. Agulia was tipped off that Fayeze and the opposing militia were at the disco. PJs team had inserted false bit coin and bank transactions into the local financial systems, knowing that they would be fed to Agulia. Agulia picked up his phone and directed a few contacts at the disco, to confront Fayeze and the opposing militia.

It all seemed surreal. But the timing, orchestration of events, setting the stage over the last two months with other influence actions that built to this crescendo, made the next steps obvious. Aguila had sent two of his key militant soldiers to take care of Fayeze, and at the same time, Aguila's militant friends engaged their opposition. The drips of gasoline were now lit, the spark lit. The high emotions and distrust led to simultaneous confrontation between the militant groups. Chaos ensued, the pulling of weapons, a gun battle. In the mix, Fayeze and several militia from both sides were killed.

The event did set off some initial reactions among the varied players, but that dissipated quickly. It was viewed as just another militia rivalry. A few of the remaining militia soldiers were arrested, and put in jail. However, Agulia was never implicated, as PJ's team also went into the varied key networks and scrubbed specific data that would have been used by investigators.



Mad Scientist Blog, January 17, 2019^x

Within three hours of his initial three am wake up, PJ had completed his mission, set in motion the events, and had his other VR team mates do cleanup by going back into the varied financial and social networks and removing any traces of the false media or financial transactions. The POTUS was briefed. Mission accomplished! The problem was permanently removed, without any loss of US life. PJ pulled off his VR/AR gear, shut down his secure electric field, and put on his running shoes. He was heading out for his usual 7 am run. Despite being tired, having that rush of adrenalin from a successful mission, he felt like running a marathon. He still had a few hours before his parents' 50th wedding anniversary.

Warfare in the future is not going to be conducted by machines, no matter how far AI advances. Warfare will instead be connected human to human, human to internet, and internet to machine in complex, global networks. We cannot know today how such warfare will be conducted or what characteristics and capabilities of future forces will be necessary for victory.

COL James K. Greer (USA-Ret.)

MAD Scientist Blog, January 17, 2019 January 16, 2019

Future Intelligence S&T Investment Roadmap 2035-2050

... four other pieces of equipment that most senior officers came to regard as among the most vital to our success in Africa and Europe were the bulldozer, the jeep, the 2-ton truck, and the C-47 airplane. Curiously, none of these is designed for combat.

Dwight D. Eisenhower

This section provides a macro overview of the major investment areas to for consideration in laying the foundation necessary to conduct and succeed in Cognitive Warfare – to enable proactive influence operations and predictive analysis. As noted previously, successful placement of such a foundation is not only an enabler for success in the competition phase, but also just as critical an enabler in the kinetic and post kinetic phases of warfare. The recommended investments will set the initial baseline foundation by 2035, and include several material and non-material areas for investment, refinement or complete overhaul. The key areas of S&T investment for the initial finding include several areas: Architecture & Infrastructure; Communication; Human Capital; Information Access & Cognition; Proactive Influence/Predictive Analysis; and Integration/Leverage.

Architecture & Infrastructure: Involves developing a fully integrated network, logistics, etc. architecture across the services, and ensuring ready access to all echelons in the rear, forward, and at the edge. A key change to our current approach to intelligence is to ensure ingest of critical types of sensor and other data (e.g., IoT, economic, social media, etc.) to enable fuller understanding of the environment and networks (human, machine, technical, social, economic, etc.). In other words, we need to flip today's current paradigm where intel data from national sources is primary, to use of open sources as primary feeder for the 85% solution in seconds which can then be shared instantly with all levels and partners. The national sources and materials added for any additional value and insights. Such an approach is critical to ensuring an OODA loop advantage.

Communication: Speaks to the physical and cultural. The physical part of communications deals with the critical need to ensure survivability, redundancy, and provide for graceful degradation in any environment. The changing the paradigm of today where there a multiple efforts to build a space communications architecture, not necessarily informed or aligned, and drive an integrated approach to ensure air, space, ground, under sea and under-ground communication are added and integrated to ensure resiliency and access. The cultural addresses the ability to understand cultural norms and unique aspects of dialect for a specific region such that the nuances to effectively conveying ideas, issues, concepts, etc. is optimized to a specific region. Just because one can collect volumes of data and information to profile a region and to enable "functions," does not equate to also being able to "communicate" effectively in a region to achieve the desired impact, effect, influence etc.

Human Capital: As discussed in the key challenges, this is a critical area, it must be addressed via expanding our coalitions, public-private partnerships, and expanding our ecosystems and integration with the private sector and academia. The reality is that relying on 1% of US population, as the basis for today's military conscription is unsustainable. We must move to invest and expand in partnerships, coalitions, new recruiting, new conscription models, etc. to expand our conscription to a minimum of 30-40%.

We must invest in new ecosystems, where we can instantaneously reach out and leverage any set of expertise across a variety of disciplines (e.g., cyber, economics, cultural, industrial, etc.). No doubt such models can be established, which build trusted networks, update and refine them, but also provide compensation. Other countries, due to lack of human capital, are expanding conscription models – such as Singapore whereby they train, educate and then move the conscripts back into the industry/commercial world. However, when a crisis occurs, there is ready access to such SMEs in minutes. Such an effort would require a significant shift in how we currently recruit, and require some significant outreach and building of networks with academia, industry, commercial and allied elements. Investments in multiple smaller pilots to assess which approaches are best, effective, are most likely to be supported by public and oversight bodies are necessary.

Information Access & Cognition: Intelligence currently focuses on collecting a lot of information, then seeking the needle in the haystack of needles. The finding suggests a different model where we begin to catalog and score information sources against the veracity, quality, volume, etc. This is a continuous job to ensure understanding and vetting of the best and most

current data sources. As required, one would tap into those sources. Given such an understanding, it is possible to begin to set profiles of normal, versus potential threat or risk situations, and thereby advance predictive analytics. Ready access to all levels of the chain of command, leveraging primary open data sources, portends to enable a game changing decision advantage for US forces. This requires another significant shift in current culture, structure and efforts. It also feeds directly into the next area of investment – proactive and predictive analysis. Financial institutions do this today, so do many other commercial entities. The plethora of data sources enable establishment of norms, setting profiles for regions, and therefore advance predictive analysis. However, in today’s intelligence arena, there are only a few such instances. Investment is required to make this the norm. Lastly, investment in integration and networks of networks (human –across industry, academia, allied, etc.) – so that one can know the unknown, share the information, collaborate expeditiously and leverage to impact mission, acquisitions, and keep pace with technology and capability development. This paper discussed this in the Future Intelligence CONOPS 2035-2050 and other areas. We must begin to invest immediately in creating this new foundation of information, but do so in a whole-of-government approach to minimize costs, duplicative efforts, and advance the greatest utility and synergy.

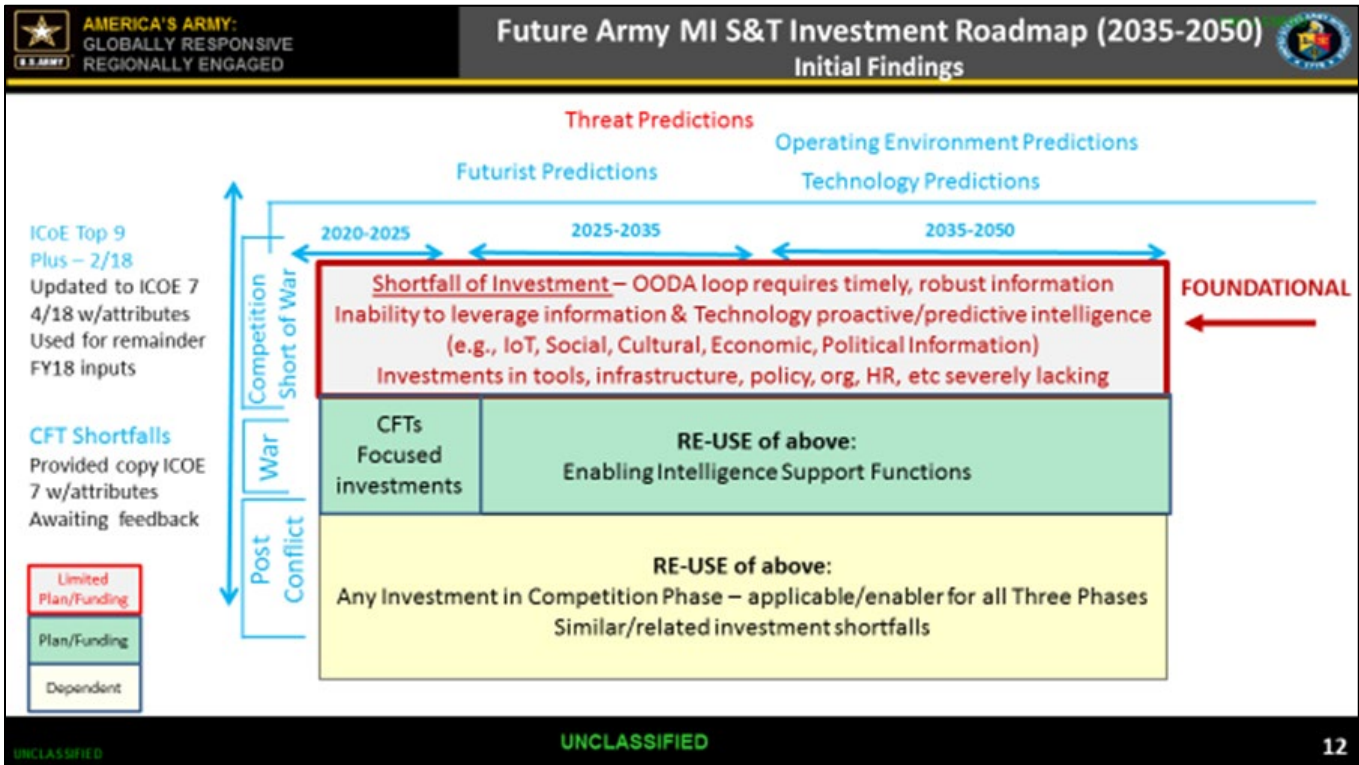


Figure 1: Future Army S&TI Investment Roadmap 2035-2050.

Figure 1 above highlights the fact that if the initial “foundation” is properly constructed, it not only serves as the key to conducting operations in the cognitive domain, but also serves to provide a pristine level of information that advances our efforts in the kinetic and post kinetic phases. And, the potential to significantly enhance the timeliness of the OODA loop is tremendous. The end game requires require an immediate rebalance of investments to ensure the cognitive is advanced in concert, and at times at a higher priority, then the kinetic investments. An increasing national debt, the costs of major weapon systems, and competition in the cognitive domain requires us to avoid falling into the paradigm, which we used to win the cold war. In other words, we must not outpace our ability to think and innovate.

We will bankrupt ourselves in the vain search for absolute security.

Dwight D. Eisenhower

Future S&T Investments 2035-2050: Examples for Consideration

This last section lays out several examples of game changing technologies.

If man does find the solution for world peace it will be the most revolutionary reversal of his record we have ever known.

George C. Marshall

First up, let's look at the Fly Wheel as an energy source. Currently the market for this capability is in the billions of dollars and expected to be trillions. Input from key vendor in this arena suggests the backlog and lucrative commercial market is so large, that it will be several years before DoD can get in the door. Living off grid, moving post/camp/divisions anywhere, powering tactical and strategic platforms are some areas that can change the dynamics of warfare. Neuro-Morphic technologies portend to inflict serious harm to both civilian and military elements of our military, diplomatic and other segments. As these capabilities develop, other countries apparently have no moral qualms about their use (e.g., used against diplomats in Cuba and China). What occurs in a decade when these capabilities are truly advanced, and they can affect legions of troops, in station, before deployment? Neuromorphic technologies are also advancing cognitive computing and decreasing the power requirements, while increasing processing power.

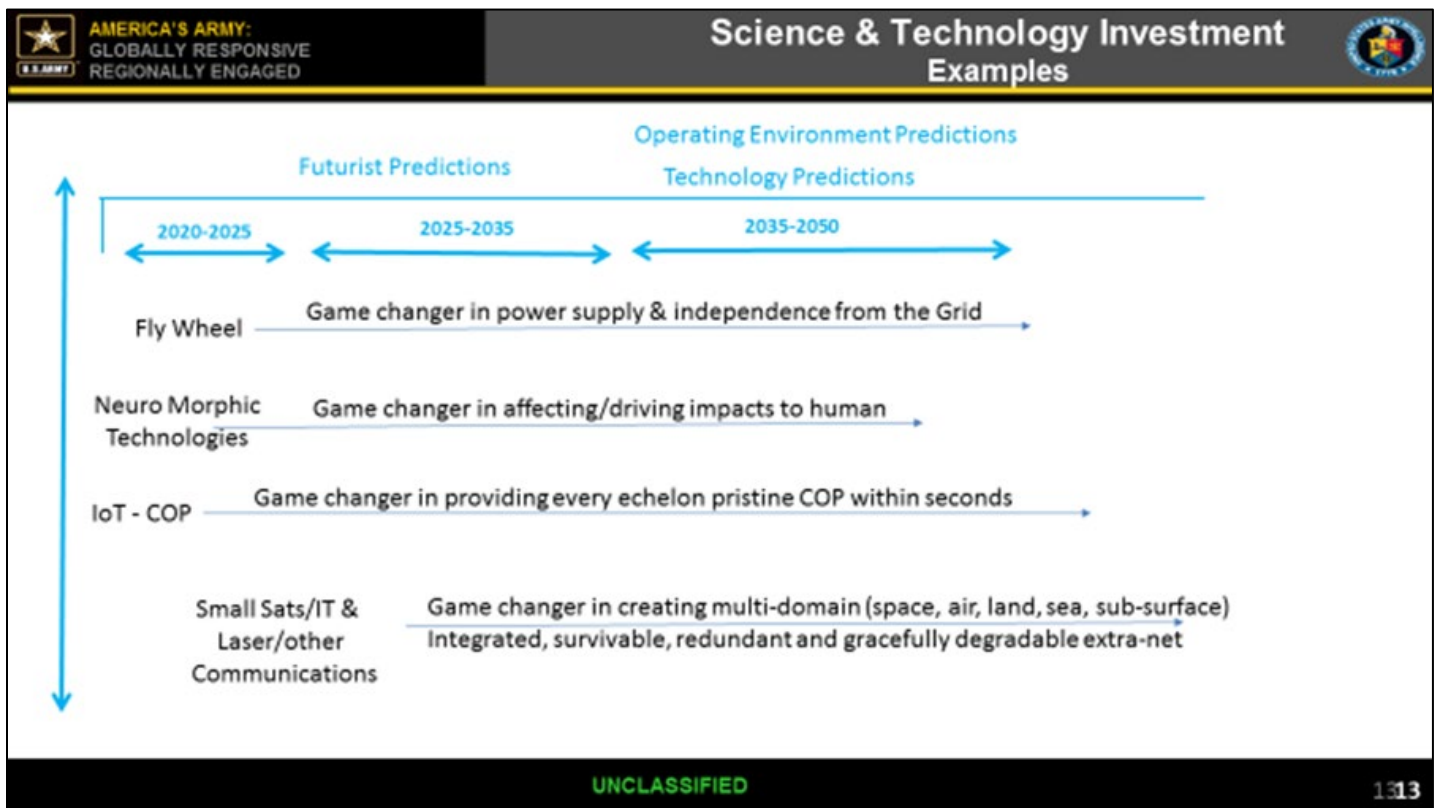


Figure 2: S&T Investment Examples

The Internet of Things (IoT) is another game changing capability that will provide both friendly and adversaries a plethora of information on our critical infrastructure, economics, social activities, movement of people, etc. that currently enables governments in assessing crises situations, flow of natural resources, details on farming, etc. In the future, this will only expand to provide a level of detail and insight into varied regions and mega cities. For example, using criminal data base information from local and national databases, IoT information, and adding in other sources, gaining a pristine view into a region or mega city will be possible.

Unfortunately, the future is real today for adversaries, not so true for our own friendly forces. The below extract from an article dealing with IoT highlights that new technologies come with both advantages as well as disadvantages.

Justin Sherman and Deb Crawford Dec 4, 2018

Industrial control systems, which command infrastructure and manufacturing processes in plants, traffic systems, and electrical grids, are increasingly “coming online” to interact with networks of small sensors and devices known as the “Internet of Things.” Together, these smaller devices and larger industrial systems form what specialists call the “Industrial Internet of Things,” and its vulnerability poses an enormous risk to national security. While cyber attacks on non-internet-connected critical infrastructure — like Stuxnet — required malicious code to be manually transferred to the victim device, hackers can now launch attacks on infrastructure remotely... The overall “attack surface” significantly increases when these connected devices are combined with older, industrial systems that themselves have terrible security.

The overall “attack surface” significantly increases when these connected devices are combined with older, industrial systems that themselves have terrible security.

The use of small satellites for communications, reconnaissance, etc. in the commercial world will enable smart cars, flying automobiles, and smarter weapons printed from simple maker kits. Figure 3, provides a list of categories and listed items that were part of a briefing put together in 2001, and projecting out to 2025 by Mr. Dennis M. Bushnell, Chief Scientist, NASA Langley Research Center. The briefing titled “Future Strategic Issues/Future Warfare [Circa 2025].” It is based on futures work with multiple DoD, IC and Federal elements. Jan 2001. It’s informative that many items are still developing and bear watching.

While enabling our forces, such capabilities also change the paradigm of conflict by also enabling the lone wolf actors. Mixing and matching such capabilities provides nation states, virtual nations, smaller groups or lone wolf actors an arsenal for good and for bad. The challenges in addressing the varied threats is exponential. Hence, chasing technology is not optimal. Keeping pace with technology is also not optimal. Keeping pace with technology and maintaining an ability for rapid adaptation, integration and adoption across the enterprise is likely to provide the greatest deterrent against varied threats.

The insights into evolving technologies drives home a reality that technology is an enabler, for both good and bad. Therefore, our best offense and defense remains proactive influence in the cognitive domain.

Our biggest challenge, is that we are in the midst of a cognitive war that will last a millennia or longer, and our focus remains near solely on the kinetic and technology.

Future Strategic Issues/Future Warfare [Circa 2025]. Dennis M. Bushnell, 2001.

Antipersonnel weaponry (neuro weapons Dr. Giordano as well)

- Heating [High Power Requirements(s)]
- Surface Effects
- Brain Interactions [Low Frequency Modulation]
- Also covered BW Acoustic

Major Influences of IT/Bio/Nano Upon Future Warfare

Ubiquitous miniaturized/networked multi physics, hyperspectral sensors

- Robotics/Automatics “in the large”
- Long range precision strike/targeting
- Info/net Warfare
- Mini/micro/nano Sats, Cruise, UAV’s
- Binary Bio Weaponry
- Miniature/ubiquitous “smart mines”

Suggested Major U.S.Future Warfare Issues

- CONUS Defense (Requirement(s) for, potential approaches)
- Logistics Defense/Protection (in/out of theater)

Future “Power Projection”?

- Humans “hold” instead of “take” ground (go in after “Sanitization”)
- Sanitization via:
 - IW/Psywar
 - Global Reach “Guns” (BWA/Slingatron)
 - Deep water/large loadout Subs w/“swimins”
 - “Robotic Everything” w/Volumetric weaponry, non-explosive warfare

- Survivability/Effectiveness of U.S. Forces on/near the “Killing Ground” in an era of affordable ubiquitous multiphysics hyperspectral sensors, precision strike, volumetric weaponry, “swarms” and hardened munitions

Figure 3: Extract from Future Strategic Issues/Future Warfare



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

SEP 15 2017

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Information as a Joint Function

Information is such a powerful tool that it is recognized as an instrument of national power. The advent of the internet, the expansion of information technology, the widespread availability of wireless communications, and the far-reaching impact of social media have dramatically impacted operations and changed the character of modern warfare.

The Chairman of the Joint Chiefs of Staff (CJCS) has issued an out-of-cycle change to Joint Publication 1, *Doctrine of the Armed Forces of the United States*, introducing *Information* as a new, seventh joint function. This change is consistent with the 2016 DoD Strategy for Operations in the Information Environment (SOIE) and the 2016 National Military Strategy. It signals a fundamental appreciation for the military role of information at the strategic, operational and tactical levels within today's complex operating environment.

The elevation of *Information* to a joint function impacts all operations and has implications across doctrine, organization, training, material, leadership and education, personnel, facilities, and policy that must be identified in the months ahead. These include the relationship with other joint functions, as well as the effects on planning and operations. The Under Secretary of Defense for Policy and the CJCS, as co-chairs of the SOIE Executive Steering Group, will lead efforts to examine implications and implement appropriate changes. I fully endorse this effort and expect support from across the Department.



03D011047-17/CMD014788-17

Appendix B: About the Author

EDWARD L. HAUGLAND

Special Advisor for Outreach & Technical ISR;
U.S. Army Intelligence/DA DCS G2

Mr. Haugland joined DA DCS G2 in July 2017 as the Special Advisor, S&T Outreach & Technical ISR, and leads an S&T Community of Interest consisting of members from the Army, IC, DoD and other Federal elements. Mr. Haugland has over thirty-five years of service in government and private sector; originally from Austin, Minnesota; and, is married to Mary Newman Haugland of Sevierville, Tennessee



EDUCATION:

CIVILIAN: BA, University of Colorado; Boulder; SE and Central European (Soviet) Studies, 1984; MA, Georgetown University; Washington, D.C.; International Affairs, 1996; Leading the Intelligence Community (SES course) Oct '16; Intelligence Fellows; Wye River, MD, 1999; Interagency Coordination NDU, 2006; Leading the Intelligence Community, October 2016; Program on Negotiation (certificate), Harvard Law School, September 2016. **MILITARY:** Squadron Officer School, USAF 1988; Defense Intelligence Advanced Sensors Training 1984; and, numerous intelligence courses.

CIVILIAN ASSIGNMENTS: 1991-1996 Industry GRCI and SWL Inc., 1996-2002 National Imagery and Mapping Agency (now NGA); DCI Community Management Staff IC CIO 1999-2000; 2002-2007 CIA; 2003 Department of Energy detail. 2007-2014 Office of the Director of National Intelligence. 2014-2017 US Army Intelligence and Security Command (INSCOM); 2017 – present Dept. Army Deputy Chief of Staff Intelligence G2.

MILITARY ASSIGNMENTS: Lowry AFB, CO Intelligence Training 1984-1985; CIA National Photographic Interpretation Center (assigned DIA, rotation) 1985-1988; Squadron Officer School 1988; On Site Inspection Agency (INF Treaty) TDY member 1988-1991; 497th Reconnaissance Technical Group USAF Europe 1989-1991; Air Force Intelligence Systems Agency (Air Staff) 1991.

AWARDS: Military included - Meritorious Service Medal, Joint Service Commendation Medal, Joint Meritorious Unit Award, Air Force Outstanding Unit Award, National Defense Service Medal, Humanitarian Service Medal and Air Force Overseas Long Tour Ribbon. Civilian included - ODNI National Intelligence Award 2013 & Integration Team Award 2014; numerous superior performance awards; NPIC 1990 Report of the Year.

- Mr. Haugland held several senior leadership positions in the ODNI from 2007-2014 that included providing recommendations encompassing the IC's collection architecture to the DNI and SECDEF; Assistant Inspector General for Inspections, Office of the IC Inspector General; and was a key architect of the IC's IPPBE processes and leading the ODNI's FY11-15 NIP programming.
- At the Central Intelligence Agency he served in several senior leadership positions that included leading CIA's Strategic Planning; deploying a major field telecommunications architecture world-wide and in war zones; and, developing CIA's first mission-based Information Technology (IT) Portfolio
- Detailed in 2003 to the DOE/IN as CIO, he led fielding of DOE's first digital imagery architecture.
- Mr. Haugland played key roles in the stand-up of the National Geospatial-Intelligence Agency (formerly NIMA) from 1996 – 2002, managing daily collection operations/placement of national collection capabilities; developing NGA's first corporate requirements processes and first Enterprise Architecture.
- From 1991-2000 he was detailed to the DCI's Community Management Staff where he served as the DCI's Representative to DoD CIO's Executive Board and played key roles in the stand-up of the first IC CIO and the successful implementation of the IC's first collaborative IT architecture.
- Mr. Haugland served in the private Sector 1991 – 1996 as Deputy Director for Business Development supporting the Office of Naval Intelligence and Ballistic Missile Defense Office (BMDO)
- He also served as a nuclear Arms Control Inspector & Deputy Site Commander in support of the Intermediate Nuclear Forces (INF) Treaty inspections in the former USSR.

Appendix C: About the Army Futures Command Community of Interest (AFC COI) & Basis and Background for Projections, Findings and Assessment

Military power wins battles, but spiritual power wins wars.
George C. Marshall <https://www.azquotes.com/quote/549970>

These projections, findings and assessments are based on my judgements alone and do not necessarily reflect those of the United States Army or Department of Defense. They are intended to set the stage for a robust set of discussions among federal, private sector and academia to inform options to advance our national security.

In addition to thirty-five plus years of experience working across the IC, DoD and private sector, the basis for the projections, findings and suggestions in the report include over three-hundred direct engagements via collaboration and discussions with industry partners/vendors, academia and with our IC, DoD, other federal partners. This includes the last 36 months of monthly Army Science and Technical Intelligence (S&TI) VTCs/meetings,

Given the Army's predominately tactical focus over the last seventeen years, it wasn't long after my arrival in August 2014 at the Intelligence and Security Command (INSCOM) that I assessed much of our intelligence Army enterprise had detached from the strategic fabric of our national security apparatus – especially the broader Intelligence Community - and had become very inwardly focused. After addressing some initial priorities, in February 2016, I began setting up a series of engagements with the Office of the Director of National Intelligence (ODNI) Director of Science and Technology (S&T), National Intelligence Managers (NIMs), and Missile Defense Agency (MDA) to introduce a small group of the original COI members. This expanded to include the Department of Energy Field Intelligence Elements (FIEs), engaging the National Intelligence Science and Technology Counsel (NISTC), to several IC, DoD and Federal agencies. Three years later, we've covered much ground, expanded our ecosystem across an all-volunteer network of participants that now reflects a "whole of government" effort to address common needs/gaps, share best practices, and advance insights into areas and efforts that inform and advance our respective missions.

The Army Science and Technical Intelligence (S&TI) Community of Interest (COI) began in February of 2016 with five Army organizations and twenty senior level personnel (INSCOM, CERDEC I2WD, PEO IEW&S, TRADOC ICOE, and DA DCS G2) involved in intelligence to achieve two objectives. First, to strategically reconnect Army intelligence to the broader national security and intelligence framework in order to leverage others investments, best practices, and insights to advance our needs/gaps; and, Secondly to provide a framework for sustained strategic engagement with our partners that is not personality based, but functions in a continuum in collaboration so it doesn't need to be reformed/rebuilt as personnel rotate. As of the writing of this white paper, February 2019, there are now seventy-plus organizations represented by over five-hundred and thirty plus members in the COI, which is transitioning to Army Futures Command (AFC). The basic purpose and objectives, and current AFC COI member list are provided in **Appendix A**.

As we began our FY2018 efforts, I was asked for two deliverables. First, to project what the Future of Army Military Intelligence (MI) would look like 2035-2050 via a Concept of Operations (CONOPS), and second to provide a Future S&T investment roadmap 2035-2050. This white paper fulfills those two deliverables. The COI was briefed on an initial set of findings in June '18. This paper is a more in-depth discussion of those findings, CONOPS and investment roadmap. It is being shared with the COI to foster continued collaboration, information sharing and strategic engagement. In December 2018, the COI began transition to Army Futures Command (AFC), and is now named the AFC COI.

The COI ecosystem (network of IC, DoD, Federal) – is really a "whole of government" network, and advancing that ecosystem to include Academia and Private sector members, will facilitate and enable an innovation ecosystem that should be replicated across varied sectors of government and our national fabric. To realize the future CONOPS and address the findings in this report requires we act, engage and operate differently. I believe ecosystems such as the COI are essential, and that sustaining and expanding such ecosystems to the private sector and academia now, ahead of other major crises, provides an expanded, trusted and proactive network of subject matter experts, diversity, and insights that truly empowers innovation, and enables people in sustaining and advancing our national security. While the COI initially focused on Army intelligence, I contend, the projections, findings, assessments and other elements of this paper apply to the broader federal enterprise, with implications for our relationships with the private sector and academia.

The COI can be viewed as counter-culture to normal mission command, given it does not direct nor action anyone, but facilitates collaboration and information sharing based on the willing input and participation of its all-volunteer membership. We question the norms, and rather than oversee or control, enable each individual member by providing them ready access to a network with insights into best practices, new technologies, and capabilities. The AFC COI provides one of the best (if not only) ready, easily sustained, network of the most diverse set of expertise and willing collaborators, innovators and self-starters across the IC, DoD and Federal government. The resulting set of SMEs provides a trusted ecosystem that can be pulsed for advice, input and understanding. As we advance each member's own organizational mission, our mission, we also advance the mission of our national security enterprise. The COI is itself a best practice, and our members exemplify the true spirit of innovation.

During the first two years of the COI, we failed to agree on a narrow focus of problem/needs. However, for our strategy in 2018, we defined a more narrow set of needs/gaps (in line with Army's priority focus on CFTs), gain inputs against those needs/gaps, and from that detail a Future S&T Investment Roadmap.

The strategy was simple, using a simple format (Figure 2) to capture a slice of the overall government portfolio that can be applied to a narrow set of needs/gaps, against a timeline that captures the projected future operating environment, threats and technology projections in the near (2020-2025), mid (2025-2035) and far-term (2035-2050). The simplicity of the Future S&T Investment Roadmap format was intended to allow all involved to understand quickly and easily discern our focus (e.g., needs/gaps), understand the threat/technology/operating environment projections, and as the roadmap was filled in – gain an insight into what Army, the IC, DoD and other Federal partners are doing that apply. In simple terms, we tried to layout a comprehensive, but focused, view of the government's investments. This was challenging, given a reluctance to share program insights or information. I call this the "Charlton Heston" effect – described later in this paper.

As the roadmap is filled in, and insights into what the government is already investing is understood, then we can begin to have a more valuable discussion with the private sector and academia. With the roadmap filled in, we can ask three critical questions to inform future investments: 1) What does the private sector or academia have that can move our current schedule to the left?; 2) What can they offer that can advance results faster, better or lower cost?; and, 3) What can they suggest that we haven't or should be thinking of, that offers a successful solution but possibly a different path or approach?

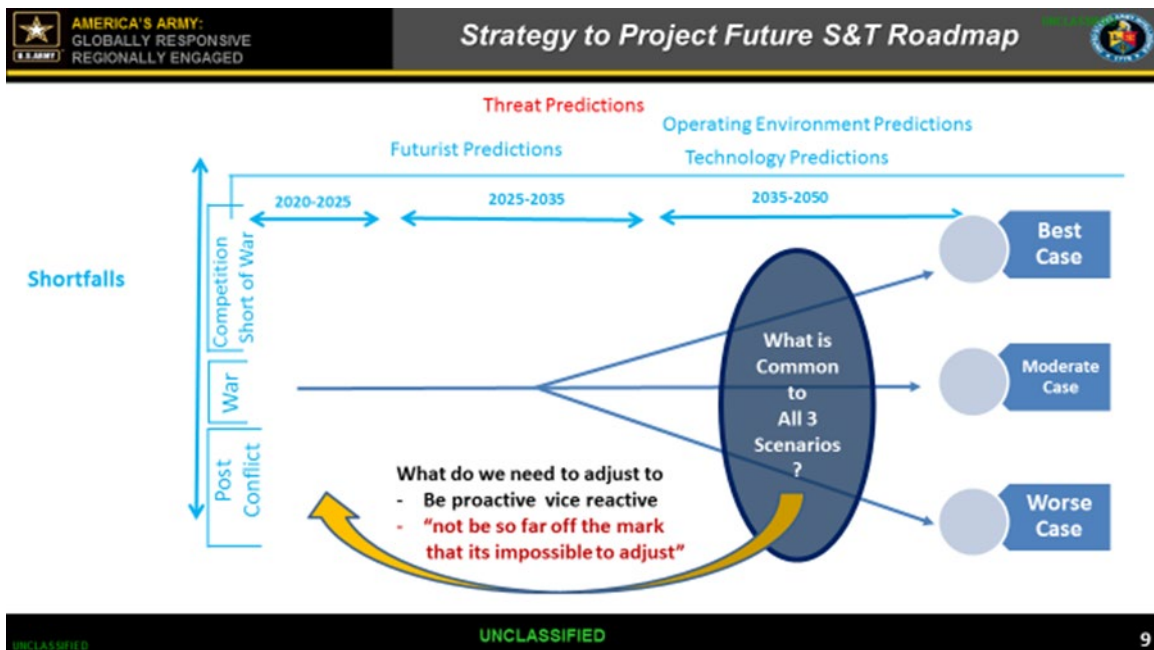


Figure 4: Future S&T Investment Roadmap 2030-2050 Format

By providing such insights and discussions, we bypass the traditional guessing game, facilitate inputs that add value vice duplicate, and can inform industry R&D investments.

I found a plethora of technology and capabilities that can be applied against any need/gap – if those needs/gaps are defined simply. Based on my experience with the COI, I contend that no matter the problem, need or gap of today, one is likely to

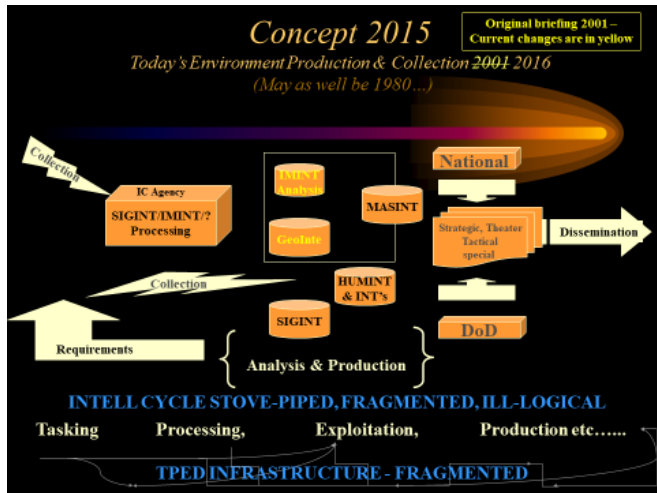
achieve at minimal a 50% solution in the next few years or better from technology or capabilities already available. The democratization of technology enables many – good and bad. In addition, it enables the inexpensive to exclusive application of technology to meet individual, nation state or varied non-state actors or virtual nations. The problem is not obtaining technology, but predicting how it will be used, how it can be used, and how to mitigate its use for nefarious reasons. Technology itself is agnostic to its use. Yet, the IC and DoD are stuck on major platform investments – while adversaries out maneuver and cause significant disruptions with low cost and expendable platforms. While there are advantages to a multi-billion dollar weapons system, when it can be defeated by a few hundred dollars and cyber intrusion – we must begin to assess our options and investments.

The synergy out of the COI VTCs was tremendous with significant interaction between our members outside of the actual VTCs. The areas we discussed covered the spectrum of warfare (competition, conflict and post-conflict phases), irregular warfare and gray zone operations, cognitive warfare, coverage of insights on best practices in organizational development; sharing of innovation and development in capabilities and S&T resulting in leveraging of other efforts to advance closure of needs/gaps beyond those in Army. We covered neuro-weapons, computing, UASs/UAVs, and had experts in discussing best practices in acquisition, prototyping, cultural mapping and unique networks, kinetic capabilities, leading edge cyber to the application and use of IoT and related data. We also covered the various “Play Books” those processes native to each service or organization used to conduct business, move money, conduct pilots, develop prototypes, etc. Traditionally most staffs know only their native playbook, these efforts broaden the insight of COI members to other playbooks they could readily access or use to advance their mission objectives. These efforts advanced synergy across and within our COI members and the varied technologies, best practices or capabilities we brought via our monthly VTCs, announcements, notes or minutes. The discussions, engagements, collaboration and information shared during these last three years provided the basis for the interim findings reported during the 18 June 2018 Army S&TI COI VTC/meeting, and inform this white paper.

Appendix D: Concept 2015

Concept 2015, created and briefed in 1999. Slide extracts are from original 1999 briefing, updates in yellow text for 2016 presentation.

Edward L. Haugland © 2019 All Rights Reserved



- ### Concept 2015 Today's Environment
- Remains SCI dominant
 - Limited Non-dominant use of open source and collateral
 - Stove-piped, duplicative, and slow
 - Quick answer in hours
 - Detailed answer in months
 - Collection quagmire
 - Multiple tools and infrastructures
 - Multiple security issues
 - Limited means to I.D. insider threat

- ### Concept 2015 Today's Environment (cont.)
- Stove-piped future slated for production & analysis
 - Desire for Collaboration, but no business process
 - More data with greater need to quickly identify, manipulate, & display info for decision making
 - Duplication/copying across tactical to national production
 - Small commercial base and reliance on SCI dominate structure threatens national security
 - Collection reflects stove-piped/fragmented production
 - Security is not full-spectrum
 - I.D. insider/outside threats not possible with current processes
 - Making little head-way
 - No common end target & cultural hurdles

- ### Concept 2015 Today's Environment (cont.)
- Majority of Data is collected, processed and analyzed in stove-pipes that are tied to Agency centric not "national/IC" data stores
 - Problems and issues tied to functional and geographic
 - via "INT" centric collection capabilities
 - limited or no with some integration of production & analysis processes
 - Reactive vice proactive priorities and tracking
 - Limited and decreasing analytical & technical base
 - Big Data "is" part of the problem - collect it all, vice collect what is smart (e.g., validated, verified, access when needed)

- ### Concept 2015 Changing the paradigm of information Tomorrow
- Geographic and functional foundation for data stores
 - Unclass and collateral dominate information holdings
 - Validation and verification to identify sources and confidence level (new profession -- info hunters)
 - 80% solution in seconds (Unclass and collateral), 95% plus solution in minutes (SCI validation)
 - Defined business processes delivers comprehensive analysis, limited production, and refined collection
 - Enhanced security control, monitoring, and impact

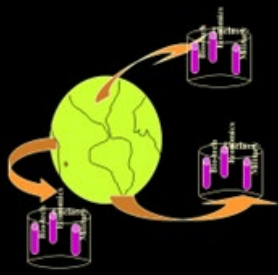
Concept 2015 Information & Data - Consciousness

- Geospatial reference
 - unique location, regional, global
 - layered data sources
- Functional reference
 - unique location, regional, global
 - layered products and information
 - inter-relation to other functional areas (one to many, many to many, or many to one)

Only so many locations - but, many ties to multiple pieces of data, information and eventually knowledge about the location

Concept 2015

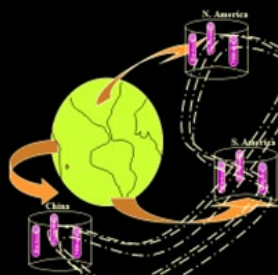
Information & Data - Understanding



- Information
 - Produced by location
 - geographic & functional
 - political, military, economic, industrial, agriculture, etc...
 - layered data
- Distinct data spheres
 - Situational awareness at multiple levels
 - status of forces, economic zones, geo-political distribution, industrial base, logistical, technical infrastructure, etc...
- Information (Consciousness) and analysis (Thought) leads to knowledge

Concept 2015

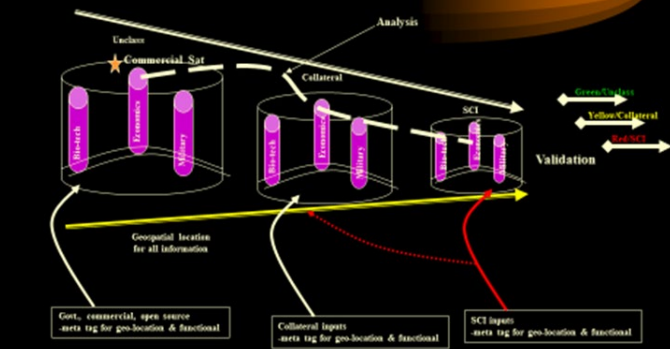
Information & Data - Knowledge & Intelligence



- Information related to one location, time, and situation equates to a “snap-shot” or picture and **consciousness**
- Information linked in bits and pieces across multiple locations, time-frames and situations through analysis equals a “flip-chart” of **understanding**
- Information that is inter-related across multiple locations, time-frames, and situations equals **knowledge and intelligence**

Concept 2015

Changing the Paradigm of Intelligence Production & Collection



Analysis

Validation

Green/Unclass
Yellow/Collateral
Red/SCI

Geopolitical location for all information

Govt, commercial, open source assets tag for geo-location & functional

Collateral inputs assets tag for geo-location & functional

SCI inputs assets tag for geo-location & functional

Concept 2015

Business Case

- **On-demand common “view”** to multiple levels of decision makers at various security levels (80-90% solution in seconds; collateral 95% in minutes; SCI level in minutes/days)
- **Refined collection** from greater number of sources
 - increased use of validated/verified open commercial sources
- **Mission focus** -- vice infrastructure & tools
 - Refine focus on numbers and types of collection assets to specific mission benefit - brunt of tasks collected commercial, tactical, theater
- **Enhanced security & detection**
 - First time audit across data domains
 - Better control of data and access across functional areas
 - Increased use of unclassified and collateral with SCI exception

Concept 2015

Business Case (cont.)

- **Increased**
 - **Collaboration** set in specific security domains
 - **National Security** through a common picture to decision makers at multiple levels (e.g., tactical to national)
 - **Retention** and utility of analysts and technical personnel
 - IT competency, senior analysts more focused
 - **Outsourcing** as required/on demand
 - IT, Analysis, production, etc...
 - **Economic benefits** potential across several fronts
 - data, tools, commercial imagery, security
 - **Analysis quality and timeliness** via better processes
 - **Collection efficiency and effectiveness**

Concept 2015

Business Case (cont.)

- **Decreased**
 - **Conflicting “views”** to decision makers
 - **Production time** (e.g., get answer and/or common “view”)
 - **Number and type of products**
 - **Infrastructure**
 - **Redundant technology efforts**
 - **Dependencies**
 - **Turn-over**

Appendix E: Enterprise Architecture Depiction

Context: Enterprise Architecture & Strategy
Enterprise Architecture

A Multi-Dimensional Problem

FUNCTION = what needs to be done, to what purpose, to what outcome

CONOPS = how you implement the functions

INFORMATION = what information is required to function

Shortfalls = what are the shortfalls to achieve desired outcome

Thesis = us & bureaucracy – not the enabling technology – will be greatest challenge

Enterprise Architecture: Is a "Living Design." It captures strategic intent, funding, the core mission and business functions, processes and underlying policies, and how they are implemented. The front end of an enterprise architecture is about the mission and intent. Only once that is defined, can it be enabled by the IT – or the backend/supporting elements or IT (systems, technical, and data) that seeks to enable, optimize and enhance.

UNCLASSIFIED 4

Ends = Strategic Intent & Objectives

Ways = Functions & CONOPS

Means = Resources (people, funding, etc.)

Note:
I've used these charts since 2001 to provide a different perspective on an Enterprise Architecture. I put forth the concept of a MEA in 2010-11.

Context: Enterprise Architecture & Strategy
What is the Minimal Essential Architecture You Need to Win?

A Multi-Dimensional Problem

TECHNOLOGY (S&T) IS AN ENABLER!

INTEGRATION = Every Enabler MUST consider interoperability, benefit, risks, and compatibility with the architecture.

What is the MEA you need to guarantee success?

Minimal Essential Architecture (MEA) is the minimum architecture necessary to fulfill an organizations' Mission Essential Functions (MEFs).

- The MEA is a sub-set of the Enterprise Architecture
- The MEA drives focus on true mission operations, priorities and investments.
- Everything over and above the MEA must demonstrate specific value, as it is less-critical by definition.

UNCLASSIFIED 5

Context: Enterprise Architecture & Strategy
Strategy Drives Outcome

Strategy - Linking the Ends to the Means

Intent drives architecture, underlined by policy, with core functions aligned by portfolios and specific resources. Resources in turn facilitate implementation of the portfolios, following policy, and guided by the architecture to realize outcomes and intent.

UNCLASSIFIED 6

Bibliography

ⁱ Dennis M. Bushnell, Chief Scientist, NASA Langley Research Center briefing “Future Strategic Issues/Future Warfare [Circa 2025]” based on futures work with multiple DoD, IC and Federal elements. Jan 2001 (references in blue color from same briefing future projections 2025)

ⁱⁱ (SECDEF Memo 9/15/17)

ⁱⁱⁱ The Strategy Bridge Strategic Design for the Complex Realm, November 28, 2018 Jeremiah Monk

^{iv} Charlton Heston was an American actor and political activist. As a Hollywood star, he appeared ... Heston was the five-term president of the National Rifle Association (NRA), from 1998 to 2003. Wikipedia https://en.wikipedia.org/wiki/Charlton_Heston

^v Article: Leap-Ahead Technologies: Could They Be the Army's Undoing?

By Matthew Cox, Military.com, April 29, 2018, *Paul Scharre, a senior fellow at the Center for New American Security.*

^{vi} Measures in Europe, Understanding the Threat; Raphael S. Cohen, Andrew Radin

Published by the RAND Corporation, Santa Monica, Calif. © Copyright 2019 RAND Corporation; www.rand.org/t/RR1793

^{vii} Nov. 5, 2018 — Colonel James “Jamie” E. Hayes III, USA, is Chief of Staff in the Deputy Directorate for Special Operations at the Joint Staff J3.

^{ix} P. 12 The Character of Warfare 2030-2050: Technological Change, the International System, and the State. Nov 2017

^x MAD Scientist Blog, January 17, 2019January 16, 2019; Today's post by guest blogger **COL James K. Greer (USA-Ret.)** Dr. Greer holds a Doctorate in Education, with his dissertation subject as US Army leader self-development. A graduate of the United States Military Academy, he has a Master's Degree in Education, with a concentration in Psychological Counseling; as well as Masters Degrees in National Security from the National War College and Operational Planning from the School of Advanced Military Studies. **113. Connected Warfare** <https://madsciblog.tradoc.army.mil/113-connected-warfare>