Digital Dimension Disruption

A National Security Enterprise Response

By Charles Rybeck, Lanny Cornwell, and Philip Sagan

The digital dimension is simultaneously enhancing and disrupting the fabric of life in every society where modern, *informatized* technology is present.[1] The slow-motion collapse of parts of the 20th century's legacy is now accelerating in ways that likely will usher in a monumental realignment of societal institutions, methods of business, and fundamental ideas about national security. This realignment will, of necessity, change the frameworks within which America provides for its security, including how it acquires the goods and services it uses in that effort.

The U.S. National Security Enterprise (NSE or Enterprise) has not yet grasped, as evidenced in budget priorities, what it means to live in a world where the threats reside at considerable distance, at scales beyond our imaginings, and at speeds that cannot be easily comprehended. Information technology has penetrated all aspects of our lives and the *informatized threat* is a clear and present danger. The People's Republic of China has penetrated our defense supply chain, North Korea has exposed our corporate vulnerabilities, and Russia has threatened our social cohesion. From a national security perspective informatized threats are by no means limited to the military or intelligence domains.

Yet the Enterprise thus far has followed predictable, requirements-driven, program-oriented constructs that attempt to "normalize" responses, which subdivides the problem too early and misjudges its scale.[2] What will it take to achieve enough common understanding to impel action? What will it take to align the NSE, its allies, and its partners to take effective, coordinated, and coherent countermeasures to maintain peace (when possible)?

The NSE needs an infusion of enterprise engineering originating within its most senior levels, to establish new rules of engagement that match the emerging threat. *Informatized conflict* redefines the battlespace and demands a comprehensive and coherent response. Success depends on the active engagement of the entire diplomatic, economic, and military arsenal. This article adopts the best current, unclassified, holistic view of an informatized era vision for the Enterprise.

Mr. Charles Rybeck, Mr. Lanny Cornwell, and Dr. Philip Sagan are senior advisors to the U.S. Intelligence Community and Department of Defense.

The Informatized Era

The word "computer" originally meant a person who did computation, like the clerks in 17th, 18th, and 19th century brokerages. Computing machines (what is now meant when anyone says "computers") emerged in the mid-20th century as a quantum leap forward in how humans did calculations and searched for information. In the past quarter century, human use of computers has changed fundamentally, but common terminology has not kept pace with reality.

Society has become almost wholly dependent on informatized systems. As part of the creative destruction/evolution that drives capitalism, the pre-informatized infrastructure has been destroyed, but societal processes—especially those of government, defense, and the law—are still those of the pre-informatized world, a world that is rapidly going out of existence. The world is using digitized, sharable information, transitioning from one-way, single-supplier siloed, one-function stovepipes to interactive ecosystems where software is orchestrating the movement of goods and services, the making of decisions, and impacting the way humans live. In just one generation, every industry has come to depend on interactive real-time decisionmaking.

A careful look at what has changed in the transition from the computer era to the informatized era reveals a qualitatively new infrastructure that matured during the past twenty years. Distance and time are compressed to the point where an adversary's geography is not decisive (or, in many cases, even discernable) and the pace of action can be so fast that it defies normal human cognition. Most U.S. citizens can identify aspects of this new infrastructure such as broadband connectivity, massive availability of compute power on a global basis via the cloud, and the advent of big data. However, the implications of the changes brought by informatization have not broken through to the thinking guiding the highest levels of the U.S. Government.

The informatized era's new infrastructure is distinguishing itself by freeing increasingly mercurial data to move around the world—from place to place, from purpose to purpose—to feed previously unimagined analytics. Indeed, the nature of data is, itself, undergoing a fundamental change. The terms "bespoke data" (from the British term for custom-tailored) and "by-product data" highlight the difference between data created in the old pre-computer and computer worlds and data created by or in the new informatized world.

Bespoke data are made by a human using measurement tools, like much of traditional intelligence, created to answer a known question. By-product data are incidentally created by machine operations, like the geolocation data dropped by smart phones, and are then available for other use. By-product data are growing exponentially as a primary feature of the informatized era, and are only in the infancy of exploitation by the NSE.

The Significance of Informatized Conflict

All informatized systems are essential to our national security irrespective of geography, or commercial or government origins. Informatized conflict includes all national security-relevant activity, both kinetic and non-kinetic, whether it is commonly understood by practitioners as being in that context or not.[3] For example, private commercial transactions are often conducted by their participants as if they had no national security implications. But all serious analysts recognize the indispensability of our critical infrastructure, including the electronic systems that facilitate commerce.

As anyone with a smart phone knows, the digital dimension is now integral to every aspect of business and societal interaction on a global scale. Viewed through the lens of informatized conflict, the "information technology" (IT) concept clearly fails to capture the full impact of the digital dimension on our world. The concept harkens back to the now-distant days when IT was a sequestered, relatively unimportant, compartment of our world. Chief Information Officers (CIOs) reported to Chief Financial Officers (CFOs) because Chief Executive Officers (CEOs) pigeonholed computers as simple aids to accounting.

While many summarize current threats under the term "cyber," a concept that points to everything digital, the terms "digital" and "cyber" are insufficient to capture the current threat dynamic. Cyber, for example, has usefully come to point specifically at computer network operations (CNO), but fails to capture the digital dimension as a whole. CNO's commonly described sub-divisions—computer network defense (CND), computer network exploitation (CNE), and computer network attack (CNA)—and encompass only a subset of the digital foundations on which modern life is being built.

Alignment—Develop Informatized Fusion

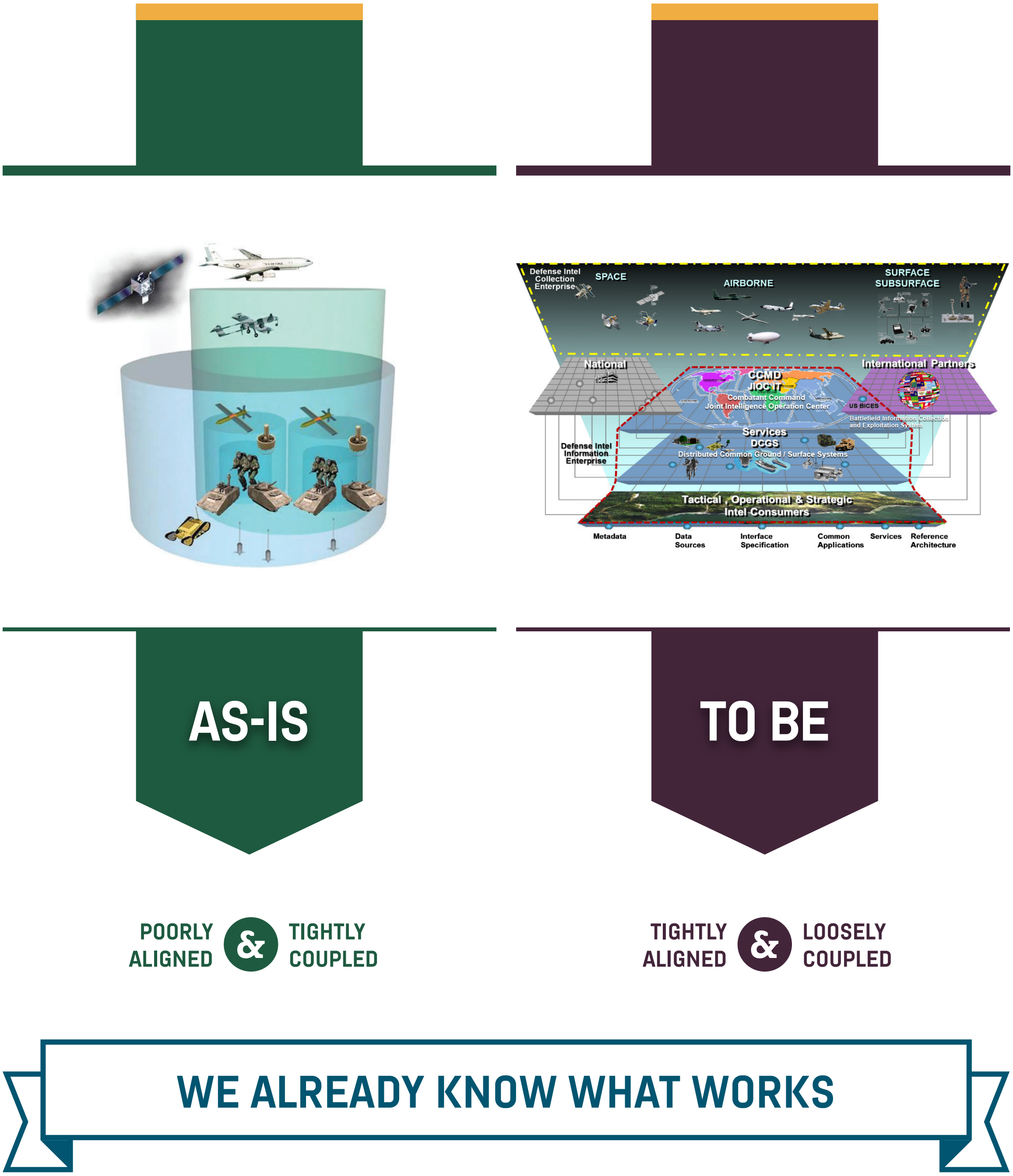
America entrusts its frontline national defense leadership to the Department of Defense (DOD) and the Intelligence Community (IC), two interconnected but separate chains of command. These entities are chartered to deliver kinetic and non-kinetic capabilities. Only the Commander-in-Chief (POTUS) controls both. As hard as it is for POTUS to exert Commander's intent, Congress faces even greater impediments when it attempts to prompt changes to how DOD prosecutes its mission. For example, Goldwater–Nichols (the U.S. Department of Defense Reorganization Act of 1986) demanded jointness in our military, and Clinger–Cohen (the Information Technology Management Reform Act of 1996) demanded IT rationalization.[4] Neither the White House nor the Congress have directed DOD or the IC with sufficient clarity to guide execution of these for the 21st century.

DOD and IC systems are compartmentalized and often impervious to improvement with industry best practices. The lefthand image on Figure 1 depicts how the NSE platforms, sensors, and weapon systems are siloed and disjointed. Every unit in the IC and DOD is sub-dividing the Enterprise problem and producing their own examples of this poorly aligned and tightly coupled approach. A massive array of programs and projects have been given carte blanche to operate using proprietary systems, creating processes that, while often narrowly effective, are impervious to improvement by informatized standards. In addition, the leaders of these programs are incentivized based on quick wins and continued resource growth, but these small pockets of capability do not add up to an Enterprise solution.

The righthand image in Figure 1 combines the vision of then Undersecretary of Defense for Intelligence James Clapper for intelligence, surveillance, and reconnaissance (ISR) with all projections of national power. This vision has not been translated into a full-blown strategy and does not yet represent the NSE reality. It does, however, provide a strong basis for the fusion of command, control, communications, computers, intelligence, surveillance, and reconnaissance.[5]

This vision of an informatized era "to be" depicts the alignment as it is required at the top and center of the Enterprise. Subsequent to that alignment, an unlimited number of loosely coupled implementations at the edge can then seamlessly connect and interoperate. This "tightly aligned/loosely coupled" engineering approach has been successfully applied at the Enterprise level in the private sector to guide foundational, internet-dependent initiatives. In less than three decades, for example, this approach has proven itself to be the most effective way for informatization to transform global enterprises, including Wal Mart, Netflix, and Google.[6] It explains not only how the internet works, but is

FIGURE 1: Tightly Aligned/Loosely Coupled as a Winning Joint Strategy.


Defense Intel Collection Enterprise
SPACE
AIRBORNE
SURFACE SUBSURFACE
National
CCMD JIOC IT
Combatant Command Joint Intelligence Operation Center
International Partners
US BICES
Battlefield Information Collection and Exploitation System
Defense Intel Information Enterprise
Services DCGS
Distributed Common Ground / Surface Systems
Tactical, Operational & Strategic Intel Consumers
Metadata
Data Sources
Interface Specification
Common Applications
Services
Reference Architecture
AS-IS
TO BE
POORLY ALIGNED & TIGHTLY COUPLED
TIGHTLY ALIGNED & LOOSELY COUPLED
WE ALREADY KNOW WHAT WORKS

ideally suited to support "innovation at the edge" for American warfighters.

Jointness in the informatized era needs to refer not only to the combined efforts of our armed services but also to the unified actions of DOD, the IC, and other stakeholders—and their ever-shifting alliances—whose efforts combine in pursuit of national security with all the instruments of national power. And fusion will need to combine data, data science, and data services to achieve the security objectives first outlined by the bipartisan 9/11 Commission.

Informatized fusion thus describes the new core competence that the NSE must develop to prevail in informatized conflict. The Chinese and the Russians have already adopted their variants of informatized fusion as guiding strategies.[7] As a democracy, however, the United States requires popular understanding and support to pursue this strategy. Fortunately, the United States variant can maintain its comparative advantage by drawing on inherent American strengths—namely constitutionally protected rights as well as checks and balances built into three branches of government, private sector competition, the rule of law, and multi-ethnic diversity.

In the words of former Director of the Central Intelligence Agency Michael Hayden, America needs to balance "unity of effort"—i.e. tight alignment—with "autonomy of action"—i.e. loose coupling. This new, agile, non-stovepiped approach to national security related actions would allow asynchronous, near real-time intervention outside today's cumbersome processes. This vision is often cited in non-authoritative documents, but it has not yet been translated into a clear Commander's Intent, Congressional Intent, or the guiding National Strategy, nor has it been realized. Unfortunately, if America stays on its present course, it is not likely to get there. Now is the time to exploit a "tightly aligned/ loosely coupled" strategy to fortify the NSE.

Mobilization—Champions Enable

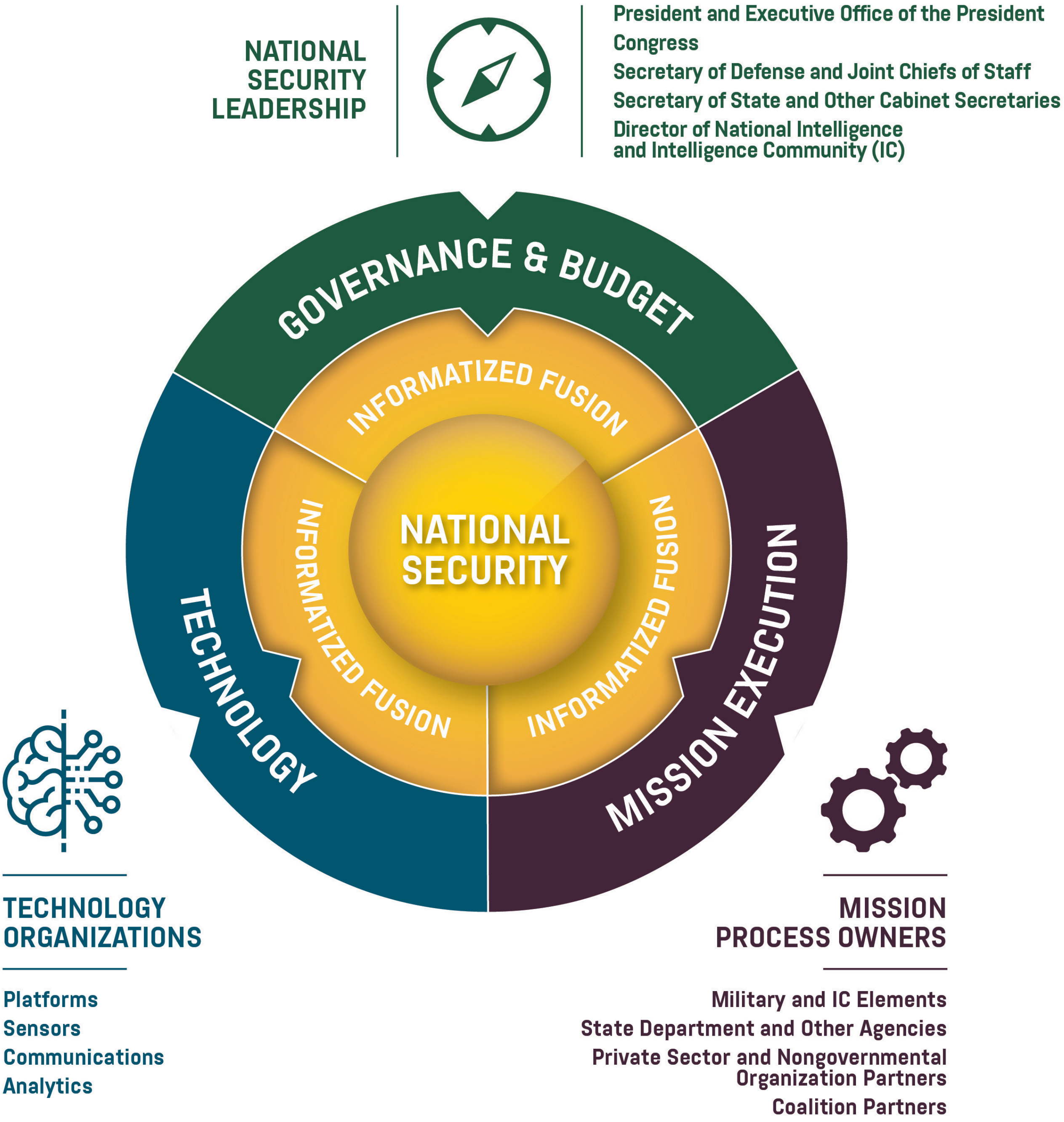
To be fair, this process has already begun at levels lower than the Enterprise as a whole, with sponsorship at lower levels and with charters, leadership, and budgets insufficient to the larger task.[9] Mission success is achieved only through authorizing initiatives at sufficient altitudes to match their charters and assigning responsibility to executives of sufficient gravitas. Informatization era challenges have their roots in the technology arena, but business-as-usual technological solutions alone will not address these challenges.

Decisionmakers and influencers from across the executive and legislative branches, with the support of the American public—will have to consider, adopt, and develop a joint 21st century vision to realize the benefits of this digital reorientation. Champions are the only ones eligible to align and mobilize in the service of jointness as redefined here to include the entire NSE.

Government governance and budget, mission execution, and technology elements perform functions analogous to their three familiar private sector equivalents—i.e. the CEO Team, the Chief Operating Officer (COO) Team, and the CIO Team. These three mission-critical teams shown in Figure 2 combine to form the NSE and fulfill its mission. Any mission-critical team can initiate Enterprise-level innovation, but it is the joint action of all three together that delivers the Enterprise-level benefits.

The differences between the government's organization and the private sector—e.g. the shared powers of Congress and POTUS—are useful in understanding why commonsense solutions and efficiencies adopted almost universally in the private sector cannot be easily adopted by the government. Informatized fusion as a joint strategy would implement mechanisms for aligning all three mission-critical areas, expedite Enterprise-level solutions, and incorporate appropriate checks and balances into the decisionmaking process.

FIGURE 2: The National Security Enterprise's Three Mission-Critical Teams.



NATIONAL SECURITY LEADERSHIP

President and Executive Office of the President
Congress
Secretary of Defense and Joint Chiefs of Staff
Secretary of State and Other Cabinet Secretaries
Director of National Intelligence and Intelligence Community (IC)

TECHNOLOGY ORGANIZATIONS

Platforms
Sensors
Communications
Analytics

MISSION PROCESS OWNERS

Military and IC Elements
State Department and Other Agencies
Private Sector and Nongovernmental Organization Partners
Coalition Partners

Ultimately, the Commander-in-Chief and Congress will need to mobilize the three mission-critical teams to meet the challenge of the digital dimension. To some observers this will look like reprogramming, to others it will present itself as major changes to mission processes, and for still others it will appear as technology transformation. To all those involved, however, it will reflect unprecedented alignment. This fusion demands cross-functional experience to fully accommodate their counterparts' frames of reference, demands, or "battle rhythms." Only a few, exceptional individuals in the government possess the required competencies—vision of the end game; cross-functional credibility; and maturity born of experience with sustained and disciplined innovation at the highest levels—to galvanize support and align stakeholders around the mission. The champions of this strategy will require a Senior Executive Technical Review and be empowered to act on its findings.[10] At the operational level, these champions will have to:

- Articulate a full-blown informatized fusion vision that matches the task and continually reminds everyone who will listen why the larger initiative is being undertaken.
- Align the vision's mission/business case (with quantitative and qualitative analysis of its risks and rewards) with its concept of operations and reference architecture.
- Arrange sufficient and sustained funding for all key elements of the initiative. Weak organizations use the mission/business case only to justify initial funding. Strong ones see a persistent, living mission/business case as a primary tool for guidance and for ensuring the delivery of promised benefits.
- Sequence activities based on announced priorities and predecessor/successor relationships to make sure benefits are delivered as promised. Only by delivering a no-kidding "without this…" list can a champion confront stakeholders with the stark reality of what it will take to achieve the benefits the champion presents in the corresponding and contingent "…you do not get that" list.
- Prioritize and communicate realistic expectations.
- Empower and incentivize executives at all levels when they enable shared, Enterprise-focused mission capabilities, and disincentivize silo-oriented approaches.

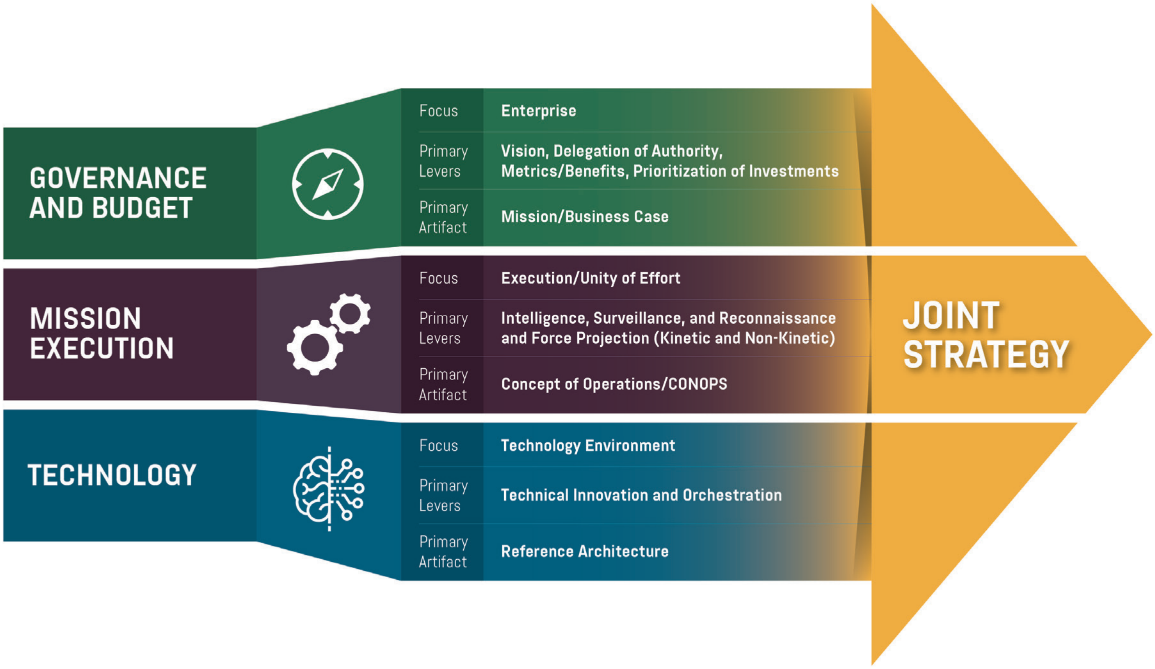
What are the Primary Levers for Informatized Fusion?

Figure 3 summarizes the NSE's response to informatization, making the "big rock" changes that the champions' levers will have to move to deliver mission benefits. The right champions will know how to use a rigorous "mission/business case" to sustain alignment among the three mission-critical teams and to sustain bipartisan support. They will need to alter the rules of engagement under which the entire NSE conducts its business.

Fortunately, the mission benefits are so powerful and the cost savings so dramatic that a coherent and well supported mission/business case at the informatized NSE level could overcome the entrenched interests who can be expected to fight it with all the tools at their disposal. Getting this right can unleash incredible growth and innovation. The potential may be compared with the 19th century commitment to build railway lines with a consistent gauge (the distance between the rails), which was an essential step in the growth to a unimodal, continental economic engine.

Many of the new rules of engagement require changes in processes where the NSE is employing 18th, 19th, and 20th century acquisition methodologies to solve contemporary, informatized problems that are mutating at an ever-increasing pace. Historic acquisition methodologies are not up to the current challenges, diminishing the NSE's

FIGURE 3: Aligning The Three Mission-Critical Teams.


GOVERNANCE AND BUDGET
Focus
Enterprise
Primary Levers
Vision, Delegation of Authority, Metrics/Benefits, Prioritization of Investments
Primary Artifact
Mission/Business Case
MISSION EXECUTION
Focus
Execution/Unity of Effort
Primary Levers
Intelligence, Surveillance, and Reconnaissance and Force Projection (Kinetic and Non-Kinetic)
Primary Artifact
Concept of Operations/CONOPS
TECHNOLOGY
Focus
Technology Environment
Primary Levers
Technical Innovation and Orchestration
Primary Artifact
Reference Architecture
JOINT STRATEGY

ability to keep up with, let alone get ahead of the rapidly rising, digitally-driven, innovation curve.

In the computer age, the NSE sought unique stand-alone things. While sometimes extraordinary, these solutions had pre-defined and relatively fixed capabilities, making them ill-suited to adapt with the changing needs of the stakeholders. In the informatized age, the focus has shifted toward integrated capabilities, solutions built on commodity technology. Even though these new informatization-aware systems are driven by specific missions, their capabilities are built to relentlessly adapt with the ever-changing needs of NSE-wide stakeholders.

Government champions as described in this article, alone, have the authority to prosecute informatized fusion and all it implies. Only they can move the biggest rocks, the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR), so that the NSE can coordinate—at the digital dimension level—procurement and deployment of virtually everything. With strong leadership, the NSE can rapidly transition from acquiring extraordinary things that confer relatively fixed capabilities to open-ended, increasingly extraordinary capabilities built using commodity things. U.S. Air Force Space Command has already begun to shift from buying rockets (things with capabilities) to buying launches (capabilities).

In the absence of fully engaged champions, the NSE routinely avoids discussion of the cross-cutting capabilities on which informatized fusion depends. Lower-level government employees are not empowered or incentivized to operate at the scale or scope required to make the needed changes in either process or procurement. They are left waiting until aligned senior executive champions intervene to exercise their extraordinary and non-routine authority, changing the rules of how business is conducted. Until then, lower-level employees are reduced to reporting classic quick wins and low-hanging fruit. Until their boss' bosses make the tough choices and substantial investments needed for informatized fusion, the oft-touted mission benefits will remain elusive.

Future Proofing the NSE

To ensure that the results of the champions' actions endure, this article looks to enterprise engineering—a discipline that makes practical application of systems engineering at the organization level, directing a venture in its entirety as a system-of-systems. It considers every aspect of the Enterprise, including business processes, information flows, material flows, organizational structure, and the human condition.

Our Constitution represents one of the most successful and earliest examples of enterprise engineering. To ensure that the NSE has the resiliency to informatized change that gives it a lifespan comparable to that of the Constitution, the NSE needs an infusion of enterprise engineering originating in the most senior levels, establishing new rules of engagement that recognize the world is now irreversibly informatized.

The history of successful reengineering of processes within the national security arena has almost invariably been associated with mission process owners who were empowered to make the necessary changes. A good—though all-too-rarely-remembered—example was provided by Admiral Hyman Rickover, the father of the Navy's nuclear propulsion program. Because Rickover was so widely respected and because his authority was so significant, he was able to serve the NSE as an invaluable counterweight to the contractors who were building the ships, ultimately forcing the adoption of the standardized solutions required to achieve Enterprise-level alignment.

Rare exceptions only prove the rule: wherever process ownership is unassigned—as it is throughout most of the NSE on most national security processes—process improvement is left homeless, without adequate guidance and context. ARPANET—the defense network that became the basis of the internet—demonstrated a means of exerting sufficient guidance and control to enhance the likelihood for success without stifiling innovation or slowing the pace of change. ARPANET offered unprecedented connectivity and revolutionized information architecture. Here the structure (packets in defined forms), flow (transmission), and management (orchestration) of information was transformed into what we all now recognize as the underlying foundation on which the modern internet is built.

Enterprise engineering has always required so much more than just managing the underlying technology. Whether dealing with the internet or the electrical grid, the private sector had to work with the public sector to set the standards. Subsequently, all enterprises (public and private) had to make major investments to adapt their business practices to take advantage of the new infrastructure.

History shows that establishing foundational alignment cannot be accomplished through business-as-usual channels. Extraordinary interventions by the most senior executives—who, under business-as-usual conditions, typically have little involvement with infrastructure—was what proved decisive. Only after alignment was achieved through regularizing the structure, flow, and management of information could the work of adapting systems for exploiting that infrastructure be delegated. In the case of informatized fusion (combining cloud, mass analytics, and the projection of national power), the NSE will need to align around changes in the structure, flow, and management of information to begin what will be an ongoing process.

The NSE's current unaligned objectives, budgets, programs, policies, and procedures limit successful examples of enterprise engineering to isolated islands. Only an "automagic fallacy" would suggest that such disparate efforts would produce informatized fusion. The NSE simply cannot afford to wait until adversaries inflict catastrophic damage before it strategically aligns and takes the steps that it already knows are needed. In advance of the unthinkable, can America do what it takes to provide for the common defense in this era of informatized conflict? PRISM

Notes

[1] Informatized is that quality—of any hardware, software, platform, sensor, process, organization, service, or device—of being digitally informed and digitally vulnerable, based on being interconnected, digitally interactive, and remotely controllable. Informatized systems are susceptible to digital input, output, influence, coordination, or orchestration, whether or not these characteristics are apparent. This article defines the term informatization and related constructs beyond their common usage by the Chinese (and beyond the original work by the Office of Net Assessment in the U.S. Department of Defense, from which the Chinese derived so much) and enhances these constructs to convey importance to our NSE. The article chose the shortened English form of the Chinese term xinxihua, "informationized" or "informatized" and combines it with "conflict." Limited and specialized terms such as "warfare," "combat," and "operations,"—the terms that the Chinese have paired with xinxihua—do not capture the ubiquity of what is being informatized. Here, "conflict" is a catchword to encompass everything involved in disputes with national security implications. For an extensive discussion of these issues: See Andrew F. Krepinevich, and Barry D. Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy*, (Basic Books, 2015).

[2] Will Roper, Ph.D., the head of the Strategic Capabilities Office in the Office of the Sectary of Defense communicated the relevant imperative succinctly as, "Don't [prematurely] subdivide the problem." Presentation at May 19, 2017 Joint Staff Industry Day held at the National Geospatial–Intelligence Agency.

[3] A 2014 paper "Military Competition and Conflict in the Information Age: Asymmetries between US and Chinese Conceptualizations of Information Operations" by Barry Watts of the Center for Strategic and Budgetary Assessment (CSBA) explores the Chinese strategic and practical insight in detail.

…The Chinese ideographs such as 信息化作战 have produced a variety of English translations, 'informationized operations' and 'informatized operations' being the most common. A more literal translation is 'information technology-based combat.'

…the US military does not have terms or overarching concepts as comprehensive, coherent and well thought through as Chinese notions of 'informationized operations' and 'informationized war' (xinxihua zhanzheng) in local, high-technology (high-tech) wars under 'informationized' conditions.

Revolution in Military Affairs (RMA) breakthroughs by the Soviet Union were studied and converted for use by the United States by Andy Marshall at the Pentagon and others in the 1970s, 80s, and 90s. These insights served as a basis for many of the US advanced technology achievements of those years. Paradoxically, the Chinese drew on and are currently drawing on the work of Andy Marshall and other Americans to develop their informatized warfare construct and strategy (what this article calls informatized fusion), while America is lagging behind.

[4] The Goldwater–Nichols Department of Defense Reorganization Act of 1986, Pub.L. No. 99–433; the Clinger–Cohen Act or the Information Technology Management Reform Act of 1996, was part of the National Defense Authorization Act for Fiscal Year 1996, Pub. L. No. 104–106.

[5] Fusion is the seamless aggregation, merging, or combination of multiple, disparate inputs into a single process for a coordinated mission purpose.

[6] Major retailers and service delivery firms (for example, WalMart in the 1990s and Netflix in the 2000s) rebuilt their supply chains using this approach. Google acquired Android in 2005. Its software, used on smartphones, tablets, and other devices, is the operating system (OS) with the world's largest installed base. Each of these businesses created a "platform" that today serves as the basis of unique business model success.

[7] For more information on China's efforts see: Fravel, M. Taylor. "China's New Military Strategy: 'Winning Informationized Local Wars'." *Browser Download This Paper* (2015).

[8] Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, (Penguin, 2016), 177.

[9] The CIA's establishment in 2015 of its Directorate of Digital Innovation (DDI), which brought the CIO and

multiple operational units together under Mission leadership) and the DNI's Intelligence Community Information Technology Enterprise initiative (which is orchestrating new infrastructure) were both examples of necessary but insufficient efforts.

[10] This "Senior Executive Technical Review" notion jars many Government leaders. There are few precedents for bringing together programmatic leads with the technical and execution leads. But without convening such expertise, the USG is left spending massively without successfully meeting the informatized conflict threat. But, acting together, the President and Congress can create this new, informatized era precedent.

Past examples are not comparable to the challenges today, but these examples are instructive. For example, Philip Zelikow brought together luminaries at the level we are proposing for the work of the Markle Foundation and the 9/11 Commission. These groups addressed complex technology and interagency challenges, translating classified and technical understandings into unclassified policy prescriptions in laymen's terms. Additionally, during World War II the U.S. President asked James F. Byrnes to leave the Supreme Court and lead what became the Office of War Mobilization in 1943.

Photos

Page 40. Image of an X-Ray Machine by Rany Montoya at the Sandia National Laboratory, available at <https://www.flickr.com/photos/departmentofenergy/8056998596/in/album-72157630137563548/>. Photo unaltered.