# Why Isn't **All Information Technology** a Matter of National Security?

*Michael R. Cirillo*

IT HAS BEEN MORE THAN TWO DECADES SINCE the terms Information Technology (IT) and Chief Information Officer (CIO) were created and one decade since "cyberspace" was established. Although the creation of cyberspace fundamentally operationalized IT and gave IT a warfighting context, the law has not kept pace. Congress also has not fundamentally operationalized the definition of IT, how we employ IT, or how CIOs function. Attempts by the Department of Defense (DoD) to affect the application of statute have only resulted in ineffective IT acquisition, cumbersome and bifurcated IT processes, and a confused paradigm for how and why we employ IT. As a nation, we have yet to come to terms with our vestigial administrative and business-like bureaucracy that prevents us from seeing IT through an operational lens, causes poor IT governance, hampers IT innovation and, most importantly, prevents the strengthening of national security.

To evolve, Congress should consider making the following changes in law:

- Enact a National Information Technology Act (NITA).
- Create an IT-type of funding that functions inside the annual federal budget cycle and update the Federal Acquisition Regulation (FAR).
- Operationalize CIOs.
- Direct centralized IT acquisition against a known IT baseline.

## Background

Federal law defines two uses of IT: National Security Systems (NSS) and Defense Business Systems (DBS). An NSS is integral to weapon systems, or used for intelligence and cryptologic activities or military command and control. A DBS is used for routine administrative and business applications. Although both definitions have undergone changes since the 1990s, to date we continue to experience strategic IT acquisition and procurement latency, an ungoverned IT procurement process, muddied operational necessities based mainly on personal IT convenience and needlessly differentiated cybersecurity.

These definitions also fail to consider that adversaries who use cyberspace against the United States seek to exploit

**Cirillo** *is an Information Technology (IT) Technical Leader and subject-matter expert at Marine Corps Systems Command. He is Acquisition Level III in IT and Program Management and a federally certified Chief Information Officer and Government Strategic Leader.*

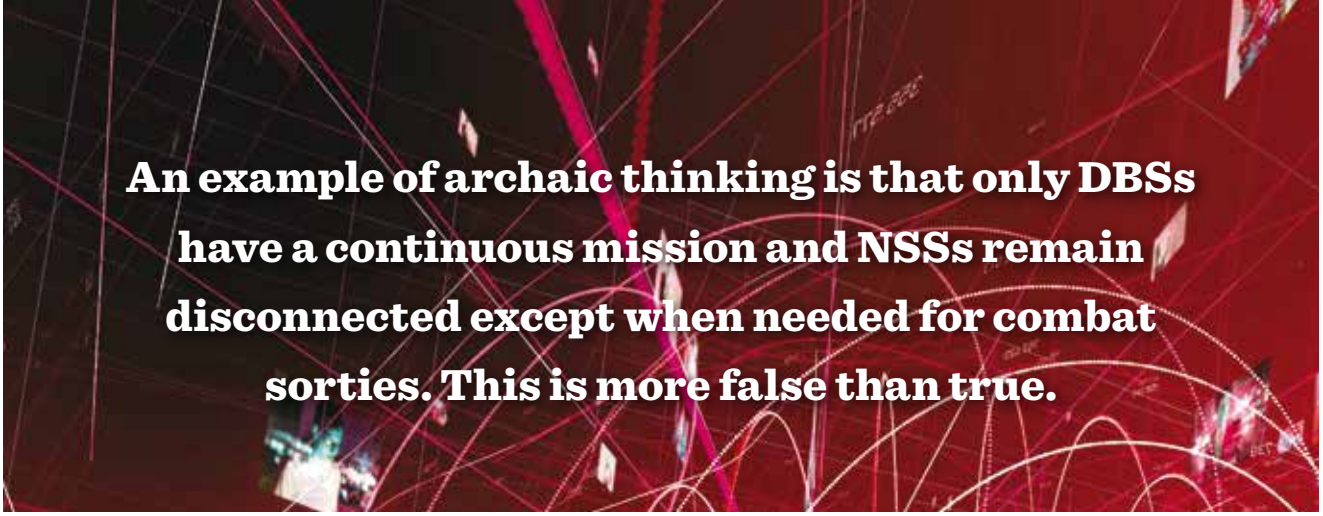
such definitional gaps in our employment of IT. Because cyberspace includes IT, both NSSs and DBSs are innately part of the same cyberspace and connect with each other. Our current mindset does not reflect the logic of this point. We remain convinced through evidence of our actions that commercial-off-the-shelf (COTS) IT is solely what we buy from big-box retailers. This consumeristic view of IT acquisition does not align with how we view acquisition of howitzers, submarines, rifles, and other military equipment. Unless we change how we view IT and begin demonstrating much greater seriousness regarding IT, the decades of compromises, data losses, stolen privacy and intellectual property, and countless IT and network failures will continue to negatively impact national security and remain a plague on the collective nature for how IT is used by our nation.

By our continued use of two definitions, we will not prevent our adversaries from taking advantage of this gap in our perspective and processes. Current statutory and regulatory guidance cannot clearly answer questions such as:

- Is a laptop cyber or IT?
- Is IT the technology and cyber the purpose?
- How does IT's cyber purpose relate to IT's uses?
- Can IT possess multiple uses? For example, can I use NSS software on a DBS laptop?
- Can I access an NSS while using a DBS?

## The Changed Landscape

In 1997, when the Clinger-Cohen Act (CCA) was enacted, having two uses for IT made sense. However, we were supposed to change our perspective when cyberspace was created circa 2009–2010. The cyberspace perspective is based on the recognition that the hyper-connected nature of information today means that adversaries, actors, entities, and others can use IT against us, that cyberspace is a contested domain like land or sea, and that harm is indeed occurring to us through the




employment of IT. In other words, cyberspace is supposed to help us understand that there is a malicious way to look at things and that using the Internet and the World Wide Web requires security, protections, verified trust, and defenses in a way not conceived of when the CCA was enacted. However, 10 years of cyber later, we have yet to adequately leverage the cyberspace way of thinking. Perhaps we have within the cyber operations community, but certainly not in general or specifically with CIO management and administrative processes.

CCA increased nonoperational and administrative IT oversight, but the creation of cyberspace as a warfighting domain should have changed this IT paradigm to one where the U.S. Government no longer views IT through an administrative lens. Despite Congress' intent, cyber-attacks have grown exponentially and computer-based viruses began negatively affecting both NSS and DBS. However, the impacts never struck a chord because they were considered an isolated event and an administrative problem.

In the late 2000s, the president and Congress slowly began to recognize threats from foreign and domestic actors seeking and gaining access into our increasingly interconnected NSS and DBS. In 2011, the DoD released its "Strategy for Operating in 'Cyberspace,'" establishing cyberspace as an operational domain. However, this strategy failed to intercede with the CIO's titled authorities, nor did it operationalize IT within a cohesive national security construct. U.S. government and corporate intellectual property remain easily removable from IT systems and—due to security updates like the 2017 patching scramble to address the Wannacry ransomware attack—we see just how far-reaching and operationally unconstrained IT's life cycle is.

The CIO's administrative and management authorities remain positioned above the command and control of cyberspace. A conflict exists between the CIO's administrative and business authorities and the operational capabilities needed to function within a cyberspace integrated with other domains, many of which also use IT. This conflict exists because our laws and regulations remain fundamentally unaffected by the adversarial nature of competing, operating, and conducting warfighting in cyberspace. This conflict has had negative impacts on government and industry IT procurement and sustainment efforts, as evidenced by DBS and NSS compromises at federal government organizations such as the Internal Revenue Service, Office of Personnel Management, and Joint Chiefs of Staff. Furthermore, national cyber operations such as Moonlight Maze and Eligible Receiver provided lessons that were misapplied or ignored.

## Archaic Thinking

In a world increasingly connected to cyberspace, we strive to evolve beyond archaic thinking and accept that IT now has a singular use relative to cyberspace. In order to remain secure amid technological improvements and rapidly changing cyber threats, all IT requires the same volume of security updates and performance upgrades.

An example of archaic thinking is that only DBSs have a continuous mission and NSSs remain disconnected except when needed for combat sorties. This is more false than true. In fact, DBSs use layered and increasingly cloud-based technology that provides different availability qualities. NSSs are increasingly connected so they can remain securely patched and ready for operations and training. Also, within cyberspace, NSSs and DBSs exist and function on an environmental scale from robust and stable to austere and unpredictable. For example, if you take a garrison laptop into combat, operate chat sessions for an operation then reach back into garrison to check payroll, you are conducting both NSS and DBS functions. In that situation, how the IT is used statutorily distinguishable as either an NSS or DBS.

We must understand the critical consequences between loss of life and business process delays. How do we compare the lost value and risk of the Office of Personal Management's data breach, when more than 20 million privacy records were stolen by foreign cyber actors, to the potential loss of life from an adversary breaching a command and control weapon system during a combat operation and reducing the number of identified enemy armored

vehicles? When measuring effectiveness, an NSS' return on investment is generally viewed through its lethality and survivability, while a DBS' return on investment (ROI) is measured through its cost benefits. With an evolved single IT use, the ROI for IT should be based on the premise of national security and independent of tactical meanings. It should be understood that acquired COTS IT, by definition, begins its life cycle already in need of sustainment.

Often, DBSs are not pure COTS and are often modified, while NSSs are increasingly tailored or pure COTS. Also, funding for IT sustainment is managed differently for NSSs and DBSs. Life-cycle funding for all IT does not include funding for patching, industry-implemented updates and unknown cyber vulnerabilities. This full life-cycle funding must be available up front; otherwise, we will continue to express feckless concern that cybersecurity gaps are not fixed immediately.

## Evolved IT Use

Across decades, incremental reform of IT acquisition has occurred with greater or lesser success. What has not occurred is an evolutionary change based upon a national security imperative. The following changes are evolutionary in nature and provide a new paradigm, identify funding changes, and foster the requisite national security and operational mindset foisted upon cyberspace by adversaries and actors.

**Congress enacts a National Information Technology Act (NITA)**. Congress should enact the NITA, which designates all IT used in, by, or for federal, state, and local government—or by any public or private entity conducting business with the U.S. government—as NIT. NITA defines NIT as a matter of national security, a potential instrument of national power requiring strategic resourcing, identically applied cybersecurity requirements and identification of "life-of-the-IT" costs for secure use. NITA fundamentally elevates the importance, relevance, and caution required for IT acquisition, operation, and sustainment.

NITA synchronizes our view of all IT as NIT, directly affected by, in and through the interconnected nature of cyberspace. All IT in the United States is nationally synchronized in cyberspace. Thinking strategically, since IT makes up the vast majority of cyberspace, Congress removes the bifurcation between IT NSSs and DBSs, or IT used in support of a weapons system. This removes the burdensome and sometimes opaque-to-industry statutes, regulations, and policies that now compel separation. This is keenly required because IT is used in the same cyberspace.

**Congress creates an IT type of funding that functions inside the annual federal budget cycle and incorporates NITA language into the FAR**. Create a cyber (IT) color of funding outside the annual federal budget cycle or inside and earlier than the 12-month cycle. A NIT color of money works less on the premise that urgency of delivery has primacy and more on the idea that technological change or enhancements in IT, and as-yet-unknown cyber vulnerabilities drive needed acceleration. Decades of IT acquisition reform by Congress have not resulted in fundamental change in the speed of IT acquisition. A reason is the lack of an express statutory mandate to enable this for IT. Because COTS IT can change so often inside the 12-month budget cycle, multiple IT needs that arise inside this budget cycle can remain unfunded for many months or cause the movement of existing funds from a currently funded need to address the emergent need. Hence, NIT having its own funding enables technology pacing in a way never before seen with multi-year funding.

The DoD's annual budget cycle has its own processes tied to the federal annual budget process. Emergent IT or emergency cyber requirements can change in months, days, or moment by moment. The absence of a statutory budget process to meet those demands results in delays in meeting operational needs such as an emergency or unimagined cyber threat, capability upgrades needed inside a planned IT refresh cycle, and a need to refresh IT in order to remain apace with a dramatic industry change. Reacting to inside-a-year needs causes organizations to jump through the proverbial hoop, jeopardize existing programs, or slip schedules across a portfolio.

Until 2016, and years after the advent of cyberspace, the FAR contained no cyber-related language. As with tanks, rifles, and ships, NIT should be procured by a single acquisition entity charged with IT acquisition under NITA. Because NITA recognizes all IT as a matter of national security, all NIT should be single-streamed to enable enforcement of enterprise standards that support IT governance, resolve training curriculum challenges, and mitigate IT sustainment problems—such as managing concerns that a contract for one type of IT does not conflict with a different contract for different IT.

**Congress operationalizes CIOs**. Recreate the Federal CIO as the National IT Advisor, place that responsibility with the National Security Council and disconnect it from its current position within the Office of Management and Budget. If a budgeting approach worked, the current status would have eliminated the above-described problems.

Require that federal department and agency CIOs report directly to department/agency heads and be responsible for department/agency IT in every capacity. Doing so reduces the vestigial Clinger-Cohen IT management and administrative authorities that have become a bureaucratic burden. Reposition DoD CIO responsibilities from the Chief

Management Office to United States Cyber Command, and move DoD's Service CIOs to Service Cyber Components, thus operationalizing IT authorities. Fundamentally, network and cyber operators need situational awareness regarding what IT was approved for acquisition along with what IT is about to be plugged into the network. CIOs placed in the cyber component merge all the requisite authorities to use IT with a national security and operational mindset. Aligning CIOs with cyberspace aligns and synchronizes the currently split awareness of IT used in cyberspace; thereby greatly enhancing situational awareness of fielded and operating NIT. NITA enables that awareness to occur prior to connection or operation.

Through NITA's operationalization of CIOs, we eliminate processes and barriers established and cemented over two decades—which created different rules, systems, and processes for DBSs and NSSs. A line would be drawn between new NIT and legacy NIT. New NIT would start fresh under the revised paradigm. Legacy NIT would be modified or gradually phased out of use. The pace of industry-driven changes to IT benefit the rapid mitigation of legacy NIT.

**Direct centralized IT acquisition against a known baseline.** As with weapon systems, Congress must direct departments, agencies, or components acquire NIT through a single organization within each department, agency, or component. This single organization must also maintain the department's, agency's, or component's NIT baseline. This NIT baseline accounts for all acquired NIT that is fielded, in operation, or in need of sustainment (refresh, upgrade, repair, etc.).

In the current situation, because of confusing federal processes regarding COTS IT, the nature of today and tomorrow's threats via IT, and the common sense that IT is a consumer item, IT acquisition and procurement is conducted by a multitude of entities within each department, agency, or component. Congress having elevated the nation's practical understanding of IT via NITA will drive the need for centralized IT acquisition and procurement. Effective control of IT purchases, employment, and sustainment does not exist at present and, given the above described landscape, the existing and mainly decentralized approach seems seriously out of touch.

In the mid-1990s, IT was purchased at the lowest level determined by IT management authorities. This highly deregulated and dispersed approach soon exposed IT inefficiencies, ineffective control of IT spending, and poor enforcement of IT standards. Because there were no federal IT baselines for measuring any defined level of performance, IT spending proliferated—some would say wildly so. And malicious intent and impacts began to demonstrate that protection of IT was at worst woefully deficient and at best rudimentary.

In the late 1990s and early 2000s, centralization of IT spending began to occur throughout the federal government, but its implementation began lagging due to a corollary effect that also was developing. There also developed a personal sense that IT use was easily and well understood—and this simply because COTS IT also was used at home and in many other non-work and non-in-extremis situations. As a result, fractures appeared in centralized IT procurement and processes were never fully implemented. And because there were almost no IT baselines, IT controls essentially did not exist.

Hence, whatever kind of IT "need" could be explained was essentially approved for employment by CIOs and this remains the process today. Had the aforementioned controls been put in place circa 2000, we would not have our current IT problems nor would we have continued to experience a large volume of malicious impacts brought about from our colloquial understanding and use of IT. Centralized IT control to an IT baseline directly improves our national security posture.

## Conclusion

In our collective minds, the IT problem remains far less important than one of national security urgency. We are lucky to have not yet experienced a monumentally expensive cyberattack. Our current bifurcated, complex, and vestigial processes hinder optimization of IT practices and diminish our national security. Our CIO-centric business management approach keeps us lulled into using an atrophied process that is inherently administrative and almost entirely void of an operational mindset and thus lacks a national security level of seriousness.

We continue to ignore many, many years of warning signs caused by globally connected actors causing billions of dollars in business losses, terabytes of stolen intellectual and technical property, and compromises to the sanctity of our personal information. Our current lackluster and consumeristic IT processes have placed the United States at a grave disadvantage in a cyber battlespace, which requires disconcertingly great competition to survive. Congress should enact NITA. Short of some terrible event, only Congress can change the nation's paradigm for how we think about IT—how we fund, buy, employ, protect, and innovate IT.

Timeliness creates relevance and, while we cannot go back in time to prevent today's problems, now is most certainly the time to fix them.

*The author can be contacted at* **michael.r.cirillo@usmc.mil**.