

Marv's Smart Future

...the future looks bright through my shades...

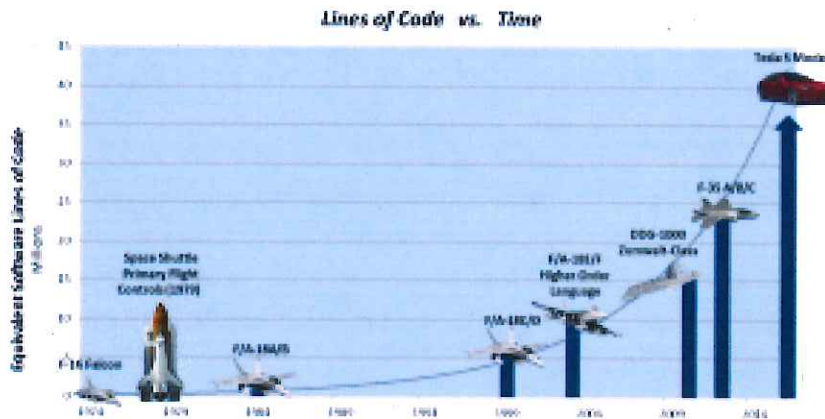
Time to Fix DoD Acquisition and Ensure Cybersecurity!

Posted on 11/23/2016 by [Marv Langston](#)

Now that we have a new administration readying to transform the Executive Branch, it is the right time to reverse decades of inefficient DoD acquisition!

Because cyber vulnerabilities are pervasive, today's acquisition challenges are even more complex than the challenges of twenty years ago. If our military systems are to remain effective at deterring and repelling foreign aggression, cybersecurity and cyber resilience must become an overriding consideration!

Recently RADM David Lewis, Commander Navy Space and Naval Warfare Systems Command, spoke at the annual Navy aviation [Tailhook Association Symposium](#). He opened his talk by telling the audience... ***...your grandmother was right, there really is a boogeyman under your bed***, and that boogeyman is cyber vulnerabilities hidden in the millions of lines of software controlling your airplane and weapon systems.



As shown by RADM Lewis' graphic above, software driven computer control permeates everything in our modern world, and for good reason. We consumers enjoy efficient and effective products at attractive prices because the




exponential growth of IT performance, coupled with reductions in IT cost, makes it logical for design engineers to embed IT into all products, from refrigerators to automobiles. That leaves only one small catch! All products and systems are now subject to cyber security attacks! A well published example is the hacked Jeep being remotely driven off the road as publicized in [Wired Magazine](#) even back in 2015.

So why haven't previous reform attempts and current DoD reforms improved acquisition effectiveness? The simple reason is that all previous and current reform



initiatives have not effectively addressed the following counter productive realities:



- **Centralized bureaucratic oversight** – continuing to bloat decision timelines, increase system costs, increase program schedule, and reduce system performance;
-  **Color of money** – slowing down development, and in turn forcing good people to invent creative time consuming ways to work around these rules;
- **High checker to doer ratio** – enabling checkers to overwhelm development and fielding decisions throughout the acquisition lifecycle;
- **Time is money** – exponentially increasing program costs in the name of taxpayer dollar stewardship, with the unintended consequence of delaying capability to the warfighters;
- **Growing cyber vulnerability** – permeating all system IT hardware and software, while cyber resilience continues to be treated as an afterthought; and,
- **DoD IT and cybersecurity arrogance and ignorance** – ignoring best commercial products and practices, while remaining years behind state-of-art cyber resilient IT technologies and products.

Based upon my 40 years of acquisition experience, I believe focusing on these three primary acquisition antagonists would mitigate these challenges:

1. **Acquisition oversight must be returned to Service level military control** where speed to capability is a cultural imperative;
2. **Cyber security and resilience must be continuously verified** rather than pacified by paper processes that leave developing and operational systems vulnerable to hackers; and,
3. **High checker to doer ratio must be reversed** to mitigate oversight second guessing by enabling trusted, but accountable, short decision cycles.

To address these realities, let's discuss **cyber security and resilience** first, because these changes could be put in place with very little Congressional involvement.

The good news:

- **Cyber Commands** have been stood up at the National and Military Service levels to actively support cyber defense, cyber offense, and cyber support to military operations;
- **Military Operational Test & Evaluation (OT&E) commands** have gotten much more engaged in cyber resilience testing which is now included, to some degree, in all system testing;
- **Cybersecurity funding** has increased significantly over the past decade; and,
- **Cyber certification** prior to system installation and operation is now the norm.

This good news, however, is overwhelmed by:

- **Ineffective cyber certification processes** further slowing development and fielding timelines; and,
- **Fast growing commercial cyber security and resilient IT hardware and software** not being quickly adopted, while DoD attempts to sustain, across its systems, end of life hardware and software.

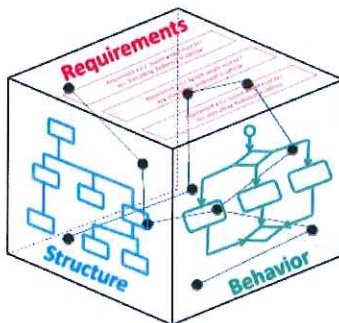
The President's new administration could reverse this reality by rapidly implementing the following changes at DoD:

1. **Transform cybersecurity from a bureaucratic approval process** into continuous or at least daily penetration testing (pentesting) and random red team activity across all DoD/IC operational system and infrastructure components.
2. **Merge DoD's Chief Information Officer (CIO) and the Principal Cyber Adviser (PCA)** positions into a single senior military CIO position, reporting to the U.S. Cyber Command, and assign senior military officers as Service CIOs, reporting to each Military Service Cyber Command.
3. **Authorize secure/resilient cyber IT system operations** following successful independent OT&E pentesting conducted by DoD and Service OT&E testers, using CIO approved pentest tools.
4. **Require daily operational IT system and infrastructure pentests** under the responsibility of operational commands, using CIO approved pentest tools.
5. **Conduct random unannounced red team events** across all DoD systems and infrastructure, conducted by the Cyber Commands.
6. **Break apart the Defense Information Systems Agency (DISA)** into a cyber resilient IT acquisition command, and an operational command reporting to U.S. Cyber Command.



The other acquisition antagonists, **oversight reform and checker doer ratio**, must be addressed from two interdependent but integrated perspectives; 1) platform/weapon acquisition, and, 2) resilient cyber IT system and embedded IT system acquisition. These changes must be supported by Congressional modifications to the Goldwater-Nichols law building from the recent good work of Senator McCain:

1. **Eliminate centralized civilian acquisition control** by re-establishing Military Service level acquisition control for all Service acquisition programs, reporting to each Service Chief; and, senior Military acquisition control for DoD Joint and Intelligence Agency acquisition programs, reporting to the Chairman of the Joint Chiefs of Staff (CJCS).
2. **Eliminate colors of money across the DoD budget**, allowing program managers the flexibility to apply all resources when and where most needed.
3. **Adopt "speed to capability" as the primary acquisition metric** for all programs across the DoD/IC and Military Services; measure performance and promotion for program managers, contracting officers, acquisition legal counsel, and financial budget personnel against speed to capability support.



4. **Apply "Model Based Systems Engineering" automation tools** to all acquisition programs using a DoD standardized tool set.
5. **Assign program managers the authority and final responsibility** for decisions that conflict with contracts and legal support.
6. **Consolidate and collapse acquisition oversight staffs** under the CJCS, and eliminate all or most staff positions from the DoD Undersecretaries of Acquisition Technology & Logistics, USD(AT&L), and Intelligence, USD(I); likewise for each of the Military Services.
7. **Eliminate most acquisition oversight decision meetings** by remotely monitoring "model based system engineering" automation tools; require meetings only when automated tools indicate high program risk or failure conditions.
8. **Establish and iterate cyber resilient IT requirements using the "IT Box" process** continuously adjusting

Agile Development Process



requirements to support operational needs; rapidly adopt new technologies that improve cyber resilience and/or operational capability.

- 9. **Acquire all IT using short cycle agile development processes and continuous user interaction** to deliver partial capability and upgrades on six to twelve month cycles.



Many would argue that DoD must be evolutionary and these suggested changes are too radical!

Decades of past and current acquisition reform, however, have delivered little value add while our military technical superiority, more than ever, is being challenged by today’s hostile and competitive global environment! Without changes like these, our Country is saddled with a DoD that pays lip-service to taxpayer stewardship, while squandering people and dollar resources on bureaucratic acquisition waste, and in response, asks its warfighters to do more with less.



At the same time, U.S. military operations have proven to the world that information dominance is a critical warfare discriminator, yet DoD acquisition worst practices are pushing U.S. military IT capabilities backward while commercial information technology is accelerating into adversary systems. For example, space based tracking and imaging, global mapping, and big data processing, are now available to anyone for a price, further eroding our U.S.

military advantage.

Now, as we enter the age of **autonomous** vehicles in the air, undersea, and on the surface, U.S. military advantage will continue to be eroded unless something is done to turn this tide.



Building upon the unforeseen election upset, a new administration is a perfect opportunity to order a “hard right rudder” on the big ship of DoD acquisition...

Posted in [Cybersecurity](#), [DoD IT Acquisition](#), [Global Perspectives](#), [Leadership](#), [Technology Evolution](#) | Tagged [cybersecurity](#), [DoD acquisition](#), [National Security](#) | [21 Comments](#)