Transforming Military Technology Through Acquisition Policy

by Rabia Altaf

The Trump administration's 2018 National Defense Strategy (NDS) emphasized the need for continued technological modernization of the U.S. Armed Forces.[324] This notion, first brought to light by the Obama administration, is underlined by the military's inability to adapt and modernize at the pace necessary to restore the United States' military dominance. At the root of this issue is the relationship between the Pentagon and the defense industry, which currently operates with an inadequate military technology acquisition process. Acquisition allows the Department of Defense (DoD) to communicate its strategic vision and shape the military to meet current and future threats. As it stands, this deficient process results in the mis-regulation of the defense industry. Improving the acquisition process by clearing hurdles, creating policy with innovation in mind, and carefully crafting regulation is critical for the United States to regain its competitive military advantage to tackle the global security issues of the coming decades. The Pentagon must also rethink its relationship with the private sector to induce more companies to join its supply chain and provide fresh solutions and perspectives to problems the United States has never faced before. As a notoriously difficult customer, the Pentagon must remove unnecessary roadblocks to attract a more diverse group of companies to supplement the defense industrial base.

Photo Montage by: William S Reeves

The Pentagon and the defense industry work hand in hand to address and maintain U.S. military preparedness, but they have also been known to bitterly disagree over the fundamentals of their relationship, especially in the domain of acquisition.[325] This friction stems from the tension between the two parties' fundamental objectives: the defense industry must make a profit in order to remain afloat, while the government must protect itself and the taxpayers' interest. These asymmetries tend to leave their disagreements at a stalemate, creating an atmosphere of distrust. Unless the Pentagon and defense industry rethink their relationship, working together to ensure the nation's military advantage will be more difficult than it needs to be.

In 1961, departing President Eisenhower warned in his farewell address, "[Government] must guard against the acquisition of unwarranted influence. . . by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist."[326] Perhaps in an effort to prevent the defense industry from wielding undue influence over the military, the government responded to Eisenhower's warning with reactive regulation that has erected onerous roadblocks and stifled industry agility and innovation. The plethora of legislative and regulatory measures is one reason the defense industry is unable to innovate quickly and successfully.[327] While defense industry support to the military is too important and too sensitive to leave unregulated, some of the last half century's regulations have missed the mark. This leaves the government overly focused on adhering to processes rather than preventing fraud, waste, and abuse. This has resulted in mis-regulation, rather than the overregulation that industry professionals often bemoan.[328] It has left the defense industry with a business model that takes years to develop, acquire, and field new technology, as well as incredibly high barriers to entry that discourage smaller companies from competing with the major defense firms.

The mid-tier acquisition (MTA) process is a recent example of DoD regulation that does not accomplish its intended objective: to allow for faster fielding and prototyping of technology to speed the pace of technological transformation. The defense industry and the Pentagon alike hoped that the 2015 passage of Section 804 of Public Law 114-92 (part of the Fiscal Year 2016 National Defense Authorization Act), establishing the MTA, would grant lower level acquisition executives the freedom to pursue faster innovation and technological advancements with their industry counterparts.[329] MTA was established to allow for rapid prototyping and fielding, enabling the government to sidestep traditional processes like milestone reviews without sacrificing the integrity and quality of the new solutions.[330] MTA's seminal feature was pushing decision-making powers down from the undersecretary level to the lower level components in the Pentagon to decide which technologies might be acquired using this method. As Burbey et al. explain:

"*Middle-tier acquisition begins with a blank slate and allows the program. . . to build an acquisition process appropriate to the capability's maturity and mission needs. This enables programs to field capabilities in two to five years. . . versus the seven to twelve years often associated with the traditional acquisition process. With middle-tier acquisition,programs can forgo the multiple checklists, signatures and annexes.*"[331]

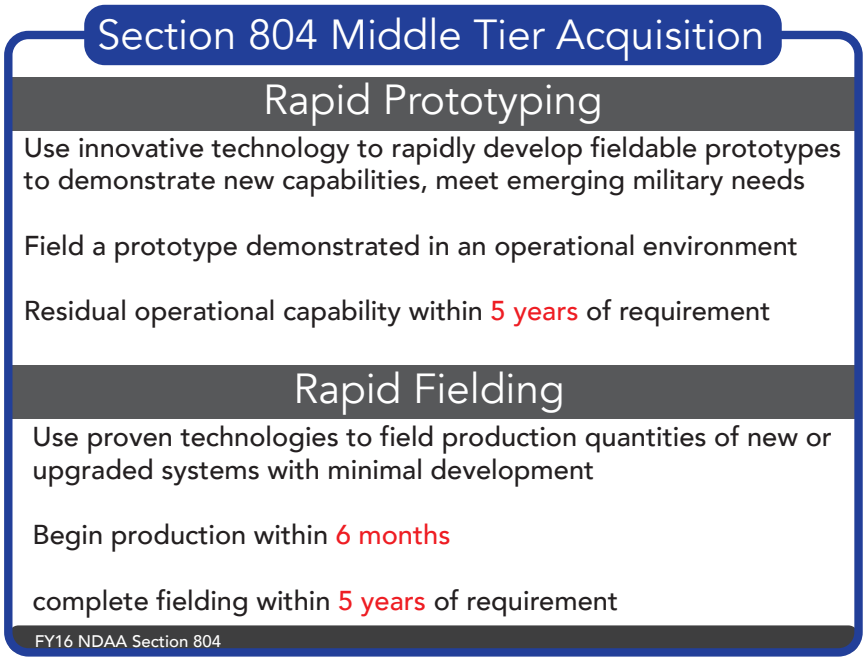

Figure 1 – MTA provisions under Section 804[332]

However, the MTA's much vaunted decision-making devolution created more bureaucratic hurdles than it intended, made worse by the Pentagon's delay in issuing guidance to its acquisition staff. The guidance delineating clear responsibilities to the staff was released on December 30, 2019, nearly four years after the law's passage.[333] As noted above, the program executive offices (or PEOs, the key offices in charge of acquisition for a particular program or programs) must create new acquisition processes related to MTA. This combination of creating their own processes while simultaneously executing them often created more confusion, especially with more parties involved. This might have been mitigated with more timely guidance.

This has led to an increased number of silos of management and information (also known as stovepipes) by including more departments of different agencies into the acquisition decision-making process. The MTA initiative did not streamline these bureaucratic processes as it purported to do. Instead, it created new ones. It also did not issue clear guidance delineating responsibilities until forced to by Congress.[334] While the Pentagon's intent in giving more power to executives closer to the acquisition process was laudable, its execution of the

MTA created confusion. More people got involved, not less, with virtually no guidance on how to manage the dramatic increase in participants. Bill Greenwalt, Senior Fellow at the Atlantic Council, said: "the document allows all different kinds of stovepipes to stick their fingers in the process. If those stovepipes . . . are too involved it could 'kill middle-tier acquisition."[335] The Pentagon understands the MTA must be better explained and implemented but has not moved fast enough to allow its acquisition personnel to take advantage of the opportunities for innovation the MTA theoretically provides. The MTA rollout is indicative of a mindset that fundamentally misunderstands the function of acquisition oversight and approval. If it does not shift this mindset, the Pentagon cannot expect to transform its military to meet the obstacles of the future that it has prioritized.

If traditional production and procurement processes are mis-regulated, then the cybersecurity realm is underregulated. The 2020 SolarWinds hack is emblematic of a beleaguered industry and government in the cyber domain. Neither industry nor government has a sophisticated or unified standard, nor capacity to anticipate attacks or identify/address systemic shortcomings, in their security hygiene.[336] The SolarWinds hack demonstrates the importance of appropriate regulation commensurate to a security threat which has regularly dominated the headlines for the past decade and puts the nation's physical and digital infrastructure security at risk. The cyber realm has the opportunity to serve as a model in functional, right-sized regulation with timely regulation and communication from the Pentagon on their needs and expectations. Piecemeal communication on implementation spread out over years, as seen with the MTA policy, will create more frustration and may lead to more dangerous cyber incursions.

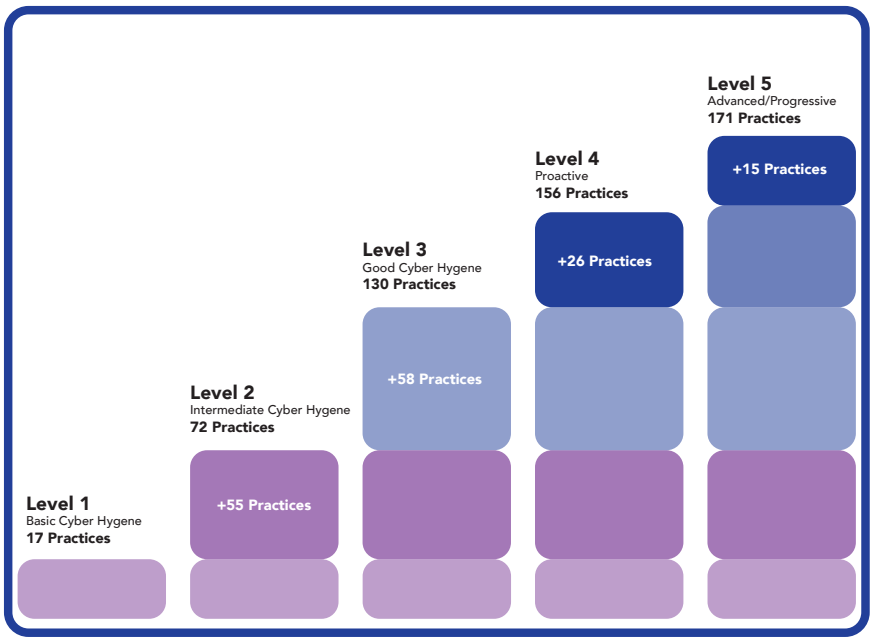

Figure 2 - CMMC Practices Per Level[342]

A recent effort toward a strengthened and unified cybersecurity standard across the DoD is the Cybersecurity Maturity Model Certification (CMMC). The CMMC is a set of DoD regulations that require contractors that possess government information to be compliant with certain standards, in other words, everything a company must do to be IT secure before even bidding for a government contract.[337] Released on January 31, 2020, CMMC contains five levels of certification. The certification requirements will follow a phased roll out over the course of five to seven years and encompasses future procedures for all contracts.[338] Certifications start from Level 1, which requires basic security hygiene such as antivirus training for employees.[339] Companies at the most advanced certification levels manage advanced persistent threats, defined as an adversary that possesses sophisticated levels of expertise and resources that allow it to use multiple attack vectors.[340] The required level of certification for a company is to be specified in the request for a given proposal and contract, which will vary based on the service or product being bid upon.[341]

The Pentagon is repeating its past mistakes (as seen with the MTA rollout) with the CMMC by not releasing guidance on reciprocity, nor communicating to the defense industry how CMMC will be implemented before the first phased rollout begins. Reciprocity policies allow for mutually interchangeable standards to be recognized by each other. With the CMMC, recognition of reciprocity would mean that similar standards already in use, such as the Federal Risk and Authorization Management Program (FedRAMP), could qualify a firm under CMMC. However, as Boyd notes, FedRAMP "look[s] at the security of products purchased by government agencies, [while] CMMC is designed to look at the companies that supply those products to ensure sensitive DOD data is safe with those vendors."[343] This means that while FedRAMP, CMMC, and other cybersecurity initiatives are similar, they do not have the same objectives. Industry firms must still submit to heavy Pentagon scrutiny to ensure equivalent compliance under CMMC, despite compliance with FedRAMP.[344] Furthermore, the investment that defense companies have made to be compliant with FedRAMP may not contribute to a company reaching the appropriate CMMC certification necessary to bid. Instead, reaching the necessary CMMC certification would require an extra cost. The company would need to spend wastefully to be compliant with almost-but-not-quite duplicative standards across the federal government. With a bit more forethought, the government could combine similar sections of standards such as FedRAMP and CMMC to eliminate as much duplicative spending as possible, rather than creating wholly different rules and certification processes.

Another pressing CMMC-related concern for the defense industry is the certification process. The Pentagon created the CMMC - Accreditation Body (CMMC-AB) to train and certify third party organizations to conduct CMMC certifications for companies. These third party organizations are meant to conduct assessments on industry's cybersecurity practices and advise companies to address identified gaps.[345] Certified assessors will then certify a company to the appropriate level. With minimum certification requirements slated to take effect in 2021, firms need to start the accreditation process as soon as possible, because the required CMMC certification must be reached at the time of bid. Rushing the accreditation process is risky because it could damage a company's chances of being eligible to bid if they are not ready in time. If companies are not eligible in time, they can lose out on business by not being able to bid at all. It could also lead to companies cutting corners to getting certified, which would undermine the objective of a unified cybersecurity standard. In shaping its acquisition policies for the cyber domain, the Pentagon has created the inverse of the problem it faced in creating the MTA program; it now does not have the administrative capacity to keep pace with its own requirements.

While the Pentagon has stated that the costs associated with reaching accreditation (such as regularly managing network or website vulnerabilities, setting up two-factor authentication, etc.) will be "allowable"—or reimbursable through allocation of the costs of the contract—these certification costs will still add a burden to the company.[346] These costs are paid up front, before any business is actually won. This means that companies may struggle to remain competitive if their prices are driven up by upfront costs that they are required to pay to become eligible for government contracts. They will only be reimbursed if they add the cost to their overhead rates, and only if they win the contract. If companies invest in the CMMC certifications but do not win enough government work to make their investment worthwhile, smaller firms may be forced to opt out of the defense industry altogether, or become prime targets for acquisition by larger prime contractors. This leads to decreased supplier diversity and other issues, as noted in 2015 by then-Undersecretary of Defense for Acquisition, Technology, and Logistics Frank Kendal, "The trend toward fewer and larger prime contractors has the potential to affect innovation, limit the supply base, pose entry barriers to small, medium and large businesses, and ultimately reduce competition—resulting in higher prices to be paid by the American taxpayer."[347]

Regulations that institute additional requirements and costs erect further barriers to entry into the defense industry. These barriers make it difficult for smaller companies to consider providing both services to the government and diverse perspectives that the Pentagon badly needs to tackle national security threats. While there are several major defense firms—Lockheed Martin, Northrop Grumman, Raytheon Technologies, L3 Communications, among others—there are hundreds of thousands of companies that act as second-tier suppliers and partners. The Pentagon would benefit from the increase in unique perspectives and solutions that a diverse pool of companies, both prime and non-prime, would provide. The technological transformation that the Pentagon needs requires a variety of companies with diversified customer experience; this can help

the DoD better understand how to tackle the threats the country faces and update military technology and practices accordingly. Current and proposed regulations work against this goal. Some, like the MTA, do not provide enough guidance to the defense industry, while others, like CMMC, do not take into account the upfront costs companies will have to pay before bidding for government work. Such mis-regulation will further inhibit the industry, stifling the transformations that the Pentagon has publicly committed itself to.

The defense sector must be able to imagine the full breadth and depth of contemporary and future threats, and innovate accordingly. In order to meet the goals outlined in the 2018 National Defense Strategy, such as countering coercion and subversion, modernizing key capabilities around situational awareness, and driving budget discipline and affordability, the United States government will have to match its acquisition processes and increase its agility to meet rapidly evolving threats and its own ambitious goals.[348] One way to begin this shift is for the Pentagon to regularly communicate its vision to the defense industry, rather than allowing years between major releases. Better guidance rollout, more thought around upfront costs, and removing barriers to entry are the foundational problems that must be addressed before the United States can expect better cybersecurity solutions and faster technological advances. This may mean engaging with more commercial and international companies to bring fresh perspectives that the American defense industry, as it currently stands, lacks.

Most importantly, the defense industry and government need a new way of thinking about their relationship in order to foster collaboration and allow for more flexibility for both parties. The government must envision and foster a diverse defense industry, outside the major companies, to ensure a greater breadth of experience and viewpoints. The present time, with a new administration and fresh challenges to address, is a prime opportunity to recreate the Pentagon-defense industry relationship to ensure a regulation and acquisition model that achieves the Pentagon's goals: efficiently transforming the military and securing our nation from the threats of today and tomorrow.

---

[324]Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
[325]Patrick M Shanahan, "Engaging with Industry" (official memorandum, Washington, DC: Department of Defense, 2018), https://www.ausa.org/sites/default/files/dod-policy-engaging-with-industry-03-02-18.pdf.
[326]Dwight D Eisenhower, "Farewell Address" (Speech, White House, Washington, DC, January 17, 1961).
[327]Richard L Dunn, "Defense Industry Needs New Way of Doing Business," *National Defense: The NDIA's Business and Technology Magazine*. 6 November 2020. Located at https://www.nationaldefensemagazine.org/articles/2020/11/6/defense-industry-needs-new-way-of-doing-business.
[328]Sandra I Erwin, "Lockheed Official: White House Looking to 'Rightsize' Defense Industry Regulations," *National Defense: The NDIA's Business and Technology Magazine*. 21 March 2017. Located at: https://www.nationaldefensemagazine.org/articles/2017/3/21/lockheed-official-white-house-looking-to-rightsize-defense-industry-regulations.
[329]Pete Modigliani, "Middle Tier Guiding Principles," *Middle Tier Guiding Principles*, Acquisition in the Digital Age - Mitre Corporation, 30 July 2018, https://aida.mitre.org/middle-tier/guiding-principles/.
[330] ibid
[331]Douglas W Burbey, Mindy Gabbert, and Kathryn Bailey, "Middle-tier acquisition authority features flexible prototype and fielding options," 12 September 2019, *US Army*. Located at: https://www.army.mil/article/227151/middle_tier_acquisition_authority_features_flexible_prototype_and_fielding_options.
[332]Pete Modigliani, Su Chang, and Dan Ward, "Middle Tier Acquisition and Other Rapid Acquisition Pathways," The MITRE Corporation, 26 June 2018. Located at: https://aida.mitre.org/wp-content/uploads/2018/06/Middle-Tier-and-Rapid-Acquisition-Pathways-26-Jun-18.pdf
[333]Scott Maucione, "DoD releases long awaited policy on mid-tier acquisition," *Federal News Network*, 3 January 2020. Located at: https://federalnewsnetwork.com/contracting/2020/01/dod-releases-long-awaited-policy-on-mid-tier-acquisition/.
[334]ibid
[335] ibid
[336]US Government Accountability Office, *Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene*, GAO-20-241, Washington, DC: GAO, 2020.
[337]For further detail, see "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," located at https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.
[338]Abigail Stokes and Marcus Childress. "The Cybersecurity Maturity Model Certification explained: What defense contractors need to know," 8 April 2020, *CSO*. Located at: https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html.
[339]ibid.
[340]ibid.
[341] ibid.
[342]University of Hawaii, "Cybersecurity Maturity Model Certification," https://www.hawaii.edu/infosec/minimum-standards/cmmc/
[343]Aaron Boyd, "Pentagon Preps for First CMMC Pilots in 2021," NextGov, Available at https://www.nextgov.com/cybersecurity/2020/12/pentagon-preps-first-cmmc-pilots-2021/170814/.
[344]Lauren C Williams, "CMMC reciprocity guidelines are still a work in progress," FCW, Available at: https://fcw.com/articles/2020/09/08/williams-cmmc-reciprocity-fedramp.aspx.
[345]Office of the Undersecretary of Defense for Acquisition and Sustainment, "CMMC FAQs," https://www.acq.osd.mil/cmmc/faq.html.
[346]ibid
[347]Jon Harper, "Defense Industry Could See Another Wave of Mergers, Acquisitions," *National Defense: The NDIA's Business and Technology Magazine*. Available at: https://www.nationaldefensemagazine.org/articles/2021/2/2/defense-industry-could-see-another-wave-of-mergers-acquisitions.
[348] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Rabia Altaf is a program manager with Raytheon Technologies. She is a 2016 graduate of The Fletcher School, having focused on business and human security. Before matriculating at Fletcher, Altaf was an intelligence analyst for the Department of the Army, conducting all-source, socio-cultural, and political analysis.

She served several customers within the Army including Training and Doctrine Command, 10th Mountain Division, and the Combined Joint Special Operations Task Force - Afghanistan. She has over a decade in experience and completed two deployments to Afghanistan in support of the U.S. Armed Forces. She is based in Tucson, Arizona.