Four Questions Indicating Unlearned Lessons Concerning Future Military Digital Systems and Fleet Design

Sam J. Tangredi, Ph.D.
CAPT, USN (Ret.)

The US military knows well that it is fully engaged in ongoing 'peacetime' cybered conflict against state and nonstate actors intending to harm the US and its allies and partners.[1] This enduring conflict is driven by various motives and takes myriad forms, ranging from ransomware attacks and theft of technical intellectual property to what is, in effect, cyber privateering and piracy. Various issues afflict the cyberspace substrate and extend deep into the socio-technical-economic system (STES) of modern Western democracies. Given the grievous damage that could be done, these vulnerabilities—many self-inflicted—are astounding.

Yet, to some extent, the US military (and perhaps its allies as well) perceives its forces and systems to be partially immune (at least internally) from these 'civilian' vulnerabilities since it has 'secure' communications, networks kept apart from the public internet, and air gaps between weapons systems and outside digital threats. But is this accurate?

Four Questions in Search of Answers and Lessons Yet to be Learned

Previous discussions in this volume prompt four questions concerning the vulnerabilities of military systems. DoD, at least in part, is addressing some of these questions. However, the scope of the vulnerabilities in the civilian socio-technical-economic system (STES), which resources our military, seem so vast as to require multiple answers (and efforts to mitigate) for each concern. The first three questions apply to all US military services, and the final question applies specifically to the U.S. Navy.

Dr. Tangredi is the Leidos Chair of Future Warfare Studies, Director of the Institute for Future Warfare Studies, and Professor of National, Naval and Maritime Strategy in the Center for Naval Warfare Studies of the U.S. Naval War College. He has wide experience as a strategic planner and director of strategic planning teams. His books include *AI at War: How Big Data, Artificial Intelligence*, and *Machine Learning Are Changing Naval Warfare*, edited with George Galdorisi (Naval Institute Press, 2021), and *Anti-Access Warfare: Countering A2/AD Strategies* (Naval Institute Press, 2013). Dr. Tangredi is a retired U.S. Navy Captain who held command at sea.

1. To **what extent is the tradeoff between security and efficiency or convenience**—the latter having rendered STES vulnerable—**creeping into the military** via adoption of current commercial business practices (e.g., just-in-time delivery), or from the small and inorganic threats that STES routinely encounters in 'peacetime' systems operations and maintenance?
2. Is the combination of threats such that **a reserve force of less digitally-dependent (or completely analog) systems** is advisable to ensure the force and fleet continuity in the highly cybered and electromagnetic spectrum-contested combat environment that will characterize any future conflict against a technological near-peer?
3. Will the contested cyberspace and electromagnetic environment **drive DoD toward autonomous systems that** operate under the concept of mission command because **we will not be able to keep the human-in-the-loop**?
4. Are the myriad digital threats such that the **U.S. Navy cannot successfully achieve the distributed maritime operations (DMO) concept** on which it expects to anchor its future fleet design? (Note: Fleet design encompasses both fleet structure and operational doctrine.)

The brief scope of this essay does not allow for answers to these questions; thorough discussion of each would require its own volume. This essay focuses on Naval lessons yet to be learned, and leaves the first three questions for the reader to ponder.

Cyber Vulnerabilities and Fleet Structure

One unlearned lesson is whether the U.S. Navy should retain less-digitized ships, aircraft, and other naval systems as an operational reserve. Arguments advanced by other experts in this collection make it unclear whether even the most highly digitized/cybered systems can themselves survive on the modern battlefield

in a conflict between technological near-peers in which cyberspace and the electromagnetic spectrum is contested. Each new capability brings new vulnerabilities—new avenues and opportunities for penetration and compromise. The greater the dependency on wireless communications within the system itself, the greater the need for (a) communications with remote offboard sensors or controls and (b) effective real time assessment of equipment status, given the greater exposure to cyber/electromagnetic penetration of those communication loops.[2]

All defense acquisition programs must now have a cyber security protection plan to mitigate cybered threats to program management, systems design, and supply chain, in order to mitigate a potential penetration of initial system acquisition. Even in the cases where these plans are in place—and many are, in reality, just risk assessments—they cannot guarantee protection throughout the lifecycle of a system that requires periodic updates, installation of new combat systems, and added commercial systems, such as low-cost navigation radars, etc.

System survivability is largely a function of two variables: vulnerability, and resilience, or bounce back. The closer a system must operate in proximity to an opponent's means to conduct the fight in the electromagnetic spectrum, the more important these factors become. Determining conclusively whether analog systems might, in fact, be more survivable in a cyberspace and electromagnetic spectrum contested environment is long overdue.

Distributed Maritime Operations - Driven to Complete Autonomy?

Another unlearned lesson is that cyber vulnerabilities could channel those operational concepts that are workable. For a critical example, cyber insecurities may prevent the U.S. Navy from achieving its goal of *distributed maritime operations* (DMO). To avoid compromising its networks via the penetration of its long-range wireless communications, may require the Navy to retain its current battle group concept of operations to allow ships unfettered communications via local networks utilizing line-of-sight UHF signals or through retransmission nodes such as drone aircraft. Without some assurance of communications continuity under battle conditions, the overall distributed network could conceivably collapse into local networks—basically independent battlegroups.

Local commanders may also be driven to authorizing more autonomy with less human-in-the-loop control or even minimizing use of key capabilities because of untrusted systems that are vulnerable to adversary meddling. Over the past several years, the Navy has presented several fleet structure plans to the Secretary of Defense and Congress that call for a larger fleet made up of a mix of manned and unmanned ships (as well as manned and unmanned aircraft).[4] This is despite insufficient open discussion of the vulnerabilities that unmanned systems will face in the real world of cybered conflict and electromagnetic warfare. How will humans retain control over these systems in a hacked environment? Manned systems will also face considerable vulnerabilities, but presumably, with crews trained to defend the critical networks and override automated control that has been electronically captured by the enemy.

How can the Navy (and DoD overall) ensure the security – and hence trustworthiness – of the hundreds of thousands of lines of code in these unmanned systems created by contracted programmers, perhaps using programs with unknown vulnerabilities? Continual inspection of code (with the added costs that requires)? How will intrusion, misdirection, or disruption be prevented in the wireless networks that provide both the sensor and commands information to the unmanned systems? These signals can be encrypted, but there are well-known difficulties in maintaining these systems' currency under the measures/counter-measures nature of warfare.

These vulnerabilities may drive the operational commanders to increase autonomy in their local area. In this circumstance, the unmanned half of the fleet will need to be to less under the direct control of 'humans in the loop' given the need to act quickly without communications prone to adversaries can disrupt or intercept. To counter command or other remote cyber intrusions, may require operations under principles of "mission command" that operate independently, with or without return to relay what they accomplished.[5]

Another aspect of this unlearned lesson is that the full implications of cyber vulnerabilities in unmanned systems are likely apparent only after they are deployed and fail operationally. Mitigating the threat and learning the lesson in advance, would require DoD policy changes,[6]and doctrinal changes in current naval warfare planning centered on fleet Maritime Operations Centers (MOCs)—perhaps proactively accepting the realities of unrestricted warfare in localized settings in anticipation of cyber-related command failures. There may be technical fixes to attempt—perhaps burst transmissions relayed via satellite to and from the autonomous platforms. However, as contributors to this volume argue, every technical fix brings its own technical vulnerabilities.[7] If the enemy can geolocate the burst transmissions, the autonomous systems become easier targets. Some argue that these vulnerabilities may be mitigated by developments in artificial intelligence (AI) systems. Yet some in this issue note that AI is linked tightly to cyber capabilities, and brings its vulnerabilities as well. Even new levels and intensity of deception need to be anticipated with rising dependence on AI.[8]

Little Hope for an Equal Field/Sea of Combat

Many contributors to this volume suggest methods by which the socio-technical-economic systems (STES) of Western democracies can be hardened and made more resilient.[9] Whether these methods are ever adopted is not a choice within the purview of the militaries of consolidated democracies. What does fall within that purview is an examination of their systems, procedures, doctrine, and force designs to seriously and routinely determine vulnerabilities that could be exploited in a conflict with a technological near-peer like China. Without doing so, there is little hope for an equal field or sea of combat. A good start in learning the lessons neglected so far would be for the Navy to grapple with and answer the four questions identified.

NOTES

1. Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age " *Strategic Studies Quarterly* 5, no. 1 (March 1, 2011).
2. There are proposals for methods to determine whether military aircraft have been hacked. See for example Marcus Weisgerber, "New Tech Aims to Tell Pilots When Their Plane Has Been Hacked," *Defense One* (web), October 4, 2019, https://www.defenseone.com/business/2019/10/new-app-tells-pilots-when-their-plane-has-been-hacked/160378/.
3. Defense Acquisition University, "Chapter 9 – Program Protection," *Defense Acquisition Guidebook*, September 22, 2020, https://www.dau.edu/guidebooks/shared%20documents/chapter%209%20program%20protection.pdf
4. On the latest iteration, see Megan Eckstein, "Navy releases long-range shipbuilding plan that drops emphasis on 355 ships, lays out fleet design priorities," *Defense News,* June 17, 2021, https://www.defensenews.com/naval/2021/06/17/navy-releases-long-range-shipbuilding-plan-that-drops-emphasis-on-355-ships-lays-out-fleet-design-priorities/.
5. See Robert C. Rubel, "Mission Command in a Future Naval Combat Environment," *Naval War College Review* 71, no. 2 (Spring 2018), pp. 109-122, https://digital-commons.usnwc.edu/nwc-review/vol71/iss2/8/.
6. Captain George Galdorisi, USN (Ret.), "Keeping Humans in the Loop," United States Naval Institute *Proceedings,* 141, no. 2 (February 2015), pp. 36-41, https://www.usni.org/magazines/proceedings/2015/february/keeping-humans-loop.
7. Giles Peeters, "A Short Burst Data Capability," *MilsatMagazine* (web), April 2013, http://www.milsatmagazine.com/story.php?number=2121128035.
8. See Sam J. Tangredi, "Sun Tzu Versus AI: Why Artificial Intelligence Can Fail in Great Power Conflict," United States Naval Institute *Proceedings,* 147, no. 5 (May 2021), pp. 20-25, https://www.usni.org/magazines/proceedings/2021/may/sun-tzu-versus-ai-why-artificial-intelligence-can-fail-great-power.
9. Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *The Cyber Defense Review* 6, no. 2 (Spring 2021).