Leading and training the "modern operator” in the information warfare age

Revenge of the Nerds: Leading and Training the “ Modern Operator” in the Information Warfare Age

“ Knowledge is power.” This quote is most often attributed to the British statesman and philosopher, Sir Francis Bacon, in *Meditationes Sacrae* circa 1597. [1] Search far enough back through historical texts and you will find the phrase used by Imam Ali as early as 10th Century and by King Solomon in the book of Proverbs. It is a widely used phrase with an insurmountable collection of interpretations. In the age of technology and the vastly expanding interconnected world in which we live, the phrase may as well be an idiom as useful as “ raining cats and dogs” or “ break a leg.” It is no longer knowledge that is the great equalizer in the instantly inter-connected, multi-domain cross-functional battlespace of the 21st Century, it is now the control of information that holds true power. Power belongs to the side who first harnesses information—whether true or not—as an instrument of war against all echelons of an adversary.

Cyberspace often times comes to mind when the term information warfare is used, but this warfighting function encompasses so much more than the cyber domain. In fact, information warfare crosses all domains of the battlespace. [2] Information warfare is all encompassing in today’s fight, which essentially extends the battlespace to nearly every corner of the world. It is because of this phenomenon that every service member should be considered—and furthermore trained—like an “ operator” deployed forward in the traditional sense. In order to establish total force readiness across all echelons for the future fight against near-peer adversaries, the DoD must

clearly define defensive information operations, and establish sound practices and policies to enable commanders to train and equip every service member as a “ modern operator.”

Using information as an instrument of war is not necessarily a new concept. According to the authors of Genesis in the Christian Bible circa 4BC, the serpent used information to manipulate Adam’s understanding of what was right and wrong, and thus led to the fall of man. [3] More recently, Russian state sponsored actors manipulated social media by circulating opposing, and many times made-up news articles. [4] Joint Doctrine defines the information environment as “ The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.” [5] Joint publications go on to describe the three dimensions of the information environment (physical, cognitive, and informational) and how information related capabilities (IRCs) are the tools and techniques that cause effects within those dimensions. [6] These are all great and relevant theories, necessary to understand offensive information warfare, but do little to highlight defensive measures of individuals and organizations.

The DoD historically has no issues relating tools of warfare to offensive effects towards an adversary. Just think rounds downrange and bombs on target. The Joint Publication 3-13 includes many diagrams, describes the ways and means of effects on critical components of an adversaries’ center of gravity, and addresses how the integration and coordination of information operations aids in achieving a Joint Force Commanders overall objectives. [7] Again, these are all well and good for aiding the Joint Staff and

leadership of information operations planning cells, but do not appropriately address the defensive information operations concerns that face service members and their families, both home and abroad. The DoD has not properly defined or identified defensive information operations, and does not have current tactics, techniques, or procedures in place to enable units and service members to properly defend themselves against information warfare campaigns.

Since the DoD has not properly defined or identified defensive information operations tactics, techniques, and procedures, it is not prepared to assemble 21st Century maneuver units to confront the changing character of war. Adversaries use tools of information warfare against service members, in the form of cyber-attacks, malicious emails, mis-information campaigns, and political warfare roughly 36 million times per day. [8] The DoD has identified that service members are not only being attacked by physical weapons of war on the battlefield, but by information weapons of war on the home front. They are even being attacked inside their own homes. Even after identifying these attacks inside the homeland, there is still a lack of focus on defensive information operations down at the unit and personal level. Mr. James Mattis is quoted in the 2018 National Defense Strategy, “ The homeland is no longer a sanctuary.” [9] While the NDS appropriately addresses the changing character of war, it does not address the concept of defensive information operations, or provide intent to subordinate commanders regarding the establishment of defensive information operations programs.

As technology rapidly improves the speed at which the far reaches the Earth communicate, the physical dimension of warfare will continue to become less targeted by adversaries. They will, in turn, continue to level the playing field by attacking in the cognitive and informational dimensions. [10] These kinds of attacks primarily occur in the “ gray zone,” which is described as “ Conflict…that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war.” [11] There is currently no in-depth or universal training for service members to prepare them for or defend against the full spectrum of information warfare. The DoD, through the service branch commanders, has an obligation to train and equip service members on what should be a newly defined front line, and shift the mindset towards training and equipping the 21st Century “ modern operator” to better prepare them to defend themselves and their families in the information environment.

There is an immediate need for the DoD to define and shift focus towards defensive information operations. With the inclusion of information as a warfighting function, a critical crusade of awareness of the implications of information warfare has slowly started to manifest. This awareness, though desperately and hastily needed across all DoD elements, must also address and define defensive information operations, as well as develop tactics, techniques, and procedures (TTPs) to facilitate individual and unit defensive postures in the gray zone. The development of established TTPs should be a bottom up endeavor, and specific to the local information environment of the unit. Division level commanders, working from higher level commander’s intent, should work with local and national level intelligence organizing to

define the information environment specific to their location. This would mirror the already established local are threat reports. Although sometimes tough to do, bilateral agreements to pass sensitive information would need to be signed. These agreements and relationships are in large part well over-due, and passing of pertinent information should become the working norm.

Policy and standardization should be studied and defined by the DoD, and outcomes should be executed through commander’s intent down all echelons. Policies and doctrinal additions would be best implemented using the centralized command; decentralized execution construct. The information environment can differ greatly from location to location, and as such, studies should be executed and evaluated locally. The results of the local studies will then be combined into the policy framework that commanders and front-line supervisors use to vector the culture of the unit and its personnel. These policies and should not be duplicative of current cyber related policies and doctrine, which focuses mainly on offensive operations, but should focus on defensive information environment posture in the gray zone and personal spaces away from home stations. These policies should also define concepts and identify tools of information warfare such as mis-information campaigns, political warfare, and a focus on using reliable and verified sources for daily news, military information distribution systems, and political polling data. The DoD defining and shifting focus towards defensive information operations will greatly aid in the protection of service members and their families. It will also enable commanders at all echelons to meet the defensive objectives set in the *2018 National Defense Strategy* .

The most critical shortfalls in the DoD’s goal of properly manning and fielding the 21st Century Maneuver Unit are the lack of defensive information operations training and front-line leadership to champion and reinforce TTPs across the total force. These shortfalls can be addressed and overcome by in-depth training and education, and a culture shift towards defensive mindedness at all levels of leadership. The DoD has not had great success with regards to defensive information warfare and/or defensive cyber operations training for individuals outside of those core military specialties. There needs to be a comprehensive rewrite and convergence of current cyber and information operations training to develop a defensive minded information operations posture. Not only should a rewrite and convergence be completed, but the entire program must be owned by commanders and enforced by front-line leaders.

Other than the occasional obligatory speech by a ranking official, article, or casual conversation, there is not nearly enough being done to highlight the importance of a defensive mindset and posture against information warfare —especially that of mis-information campaigns and political warfare targeting election related information. A Ground Combat Element of the Marine Air Ground Task Force (MAGTF) tasked with defense of an objective would not allow weak and nearly non-existent hardened defensive fighting positions. An Expeditionary Fleet Commander would not stand for weak boundaries and loose lines between ships. A C-17 Flight Commander would not lead their elements into contested airspace without fighter escorts and suppression of enemy anti-air capabilities. If these concepts of defense are

doctrinal and nothing less is to accepted, the risk of a weak defense in the information environment also cannot be tolerated.

An obvious objection and counter to shifting focus towards defensive information operations would be the long contract cycle for development of training, along with the addition of training overhead for units. “ How many more Computer Based Training (CBT) are we going to have” and “ Troops spend more of their day completing CBTs than they do actual work” are very common sentiments expressed during command climate surveys across the DoD. While this is a valid argument, it does not address the root problem—history of poorly written contracts that have resulted in poorly developed CBTs. Statistics and results of DoD CBTs across the board are difficult to find, and even when found vary widely to the point of an unacceptable margin of error. [12] If awareness is the only goal, it is possible for a CBT to reach that goal with a majority of intended targets. With the shift of focus towards defensive information operations for individuals, awareness is not the only goal. Awareness is an integral part, but the training must go deeper than a 45-minute CBT. The shift must become part of the unit’s standard operating procedure, and moreover it’s identity. To accomplish this, a mix of CBTs, 360-degree supervisor discussions, practical applications, and honest and accurate metrics will need to be established. Most of all, commanders will be the cornerstones of the shift. They will need to step up and drive the process to ensure every troop is well-equipped and prepared to defend themselves in the information environment. So, no this is not just another CBT. This is a total shift of focus towards one of the most overarching 21st century adversary threats and an establishment of a new way of operating in the

expanded battlespace that has transgressed the traditional physical boundaries. The transgression has essentially converted every individual a “ modern operator.”

In conclusion, the DoD must refocus information operations efforts towards defining and building a strong defensive posture. This is imperative in re-shifting the baseline of correct and reliable information, and how service members protect themselves and their units against adversaries using mis-information or political warfare campaigns to target in the Gray Zone. Once relevant and effective training and TTPs are developed, it will be essential for front-line leaders and unit commanders to champion the program. Much like the top-down planning process, commanders will guide and drive this program. In the end, the identified critical shortfalls will be filled. This will aid in facilitating the right combination of personnel, multi-domain capabilities, and technological understanding is used to man the agile, lethal, and resilient 21st Century Maneuver Unit.

NOTES

1. Sir Francis Bacon, *Meditationes Sacrae* (London: Londini Press, 1597).

2. Joint Staff Director for Operations, *Joint Publication 3-13: Information Operations* (Washington, DC: 2014), I-2.

3. Gen. 2: 4-3: 24 (New International Version)

4. Craig Timberg and Tony Romm, “ New Report on Russian Disinformation, Prepared For The Senate, Shows the Operation’s Scale and Sweep,” *The Washington Post,* December 17, 2018, https://www. washingtonpost.

com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/? noredirect= on&utm_term=. 9a6417b4de3f.

5. Joint Staff, *Joint Publication 3-13,* I-1

6. Ibid., I-2, 3, 4.

7. Ibid., II-1, 2.

8. Frank Konkel, " Pentagon Thwarts 36 Million Email Breach Attempts Daily," *Nextgov,* January 11, 2018, https://www. nextgov. com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/.

9. U. S. Department of Defense, *2018 National Defense Strategy* (Washington, DC: Office of the Secretary of Defense, 2018), 3.

10. Unknown User, " The Changing Character of Warfare: Takeaways for the Future," *Mad Scientist Laboratory,* April 9, 2018, https://madsciblog. tradoc. army. mil/43-the-changing-character-of-warfare-takeaways-for-the-future/.

11. Hal Brands, " Paradoxes of the Gray Zone," *Foreign Policy Research Institute,* February 5, 2016, https://www. fpri. org/article/2016/02/paradoxes-gray-zone/.

12. Chad Garland, " Air Force Slashes Computer-based Training Requirements," *Stars and Stripes,* May 8, 2018, https://www. stripes.

com/news/air-force-slashes-computer-based-training-requirements-1.

525885.