Cyber Deterrence – Article Review

This article is very helpful in defining the terms and discussing the complexities of deterrence in cyberspace. After reading the article I understand much more about the United States cyber deterrence strategy and where some of the holes exist today. Cyber deterrence is a balancing act between passive and active deterrence. “Finding the proper mix of passive and active actions is the key to building a successful strategy” (pg 3). Passive deterrence boils down to a strong defensive capability, while active deterrence boils down to a strong offensive capability.

According to the policy in this area, the US is currently relying on passive strategies to produce deterrence in cyberspace. However, Col McKenzie argues, “Passive cyber deterrence (deterrence by denial) alone will not inflict the necessary fear in an adversary to prevent attacks. There must be a credible threat to impose an undesirable set of penalty measures to have a successful and effective strategy” (pg 3). One key fact here is credibility. Will Goodman, in his article titled *Cyber Deterrence: Tougher in Theory than in Practice?* describes credibility in the realm of deterrence to be “the attacker’s calculation of the defender’s capability and intent to carry out the deterrent declaration and whether the deterrent measures can be contested.” For other states to receive a deterrent declaration as a serious threat, the declaration must be credible and believable.

The importance piece here is that once we draw a line in the sand, we have to be ready to act with decisiveness once another state or actor crosses the line. However, this retaliatory action is difficult for many reasons. First, if the retaliation is in the cyber realm, national decision makers may not want to expend a cyber weapon after a line is crossed. There are vast complexities behind the employment of a cyber weapon, which is discussed later in the article on page 7 and in other links on the Cyber Education Hub (search for “Cyber Weapons”).

Another issue that Col McKenzie discusses is the difficult task of defining a cyber-attack. What would cross the line in cyberspace. To help us understand, he included a helpful figure to aid our understanding of where the line might be drawn. The figure captures the spectrum of cyber operations and groups the actions into three categories: (1) access operations, (2) cyber disruption, and (3) cyber-attack. This breakdown is very helpful for cyber operators and those thinking about where to draw a line in cyberspace.

Additionally, cyber deterrence depends on attribution. To successfully respond to a cyber-attack, the attack must tracible to a specific actor or state. If the identity of the attacker cannot be determined, then deterrence begins to break down because we don’t know who to attack back.

The discussion on cyber policy outlines several crucial points, providing strong evidence that our national cyberspace policy, particularly in the area of deterrence, needs to be updated. However, I don’t believe this can happen until the nation as a whole, and the military in specific, evolve our thinking concerning cyber warfare. Additionally, I believe the country needs to be able to be willing to draw a line somewhere and then seek to follow through on the promises (threats) we make using the complete DIME model of influence (Diplomatic, Information, Military, and Economic). Col McKenzie closes his article by emphasizing his view that the US can and should have a viable deterrence strategy, but the current actions are not enough to produce the desired effect. If we can evolve our thinking in this area, and then respond consistently and appropriately depending on the attacker or actor, then we will be moving closer to an effective cyber deterrent.

Will Goodman’s article (Cyber Deterrence) can be downloaded here: <https://www.jstor.org/stable/26269789?seq=1#metadata_info_tab_contents>