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>

Social Engineering (Phising Attacks) - Review

<https://www.wombatsecurity.com/news/social-engineering-how-social-media-compounding-threat>

Note: The first bullet in the middle of the article should read “More than $5B in global losses in 131 countries between October 2013 and December 2016.”

This article is written to describe the connection between social engineering and social media. What is important to note is the growing percentage of monetary loss by companies in the last 5 years. This is money that is going directly to cybercriminals. The attacks are so effective because they impersonate executives or other trusted authority figures. This works because people are conditioned to say “yes” to authority figures. Wire transfers are not typically executed in the military, so this means a lower chance of this type of social engineering attacks yielding a payout for the attackers. However, there are other attacks that could target the rigid authority structure in the military leading to other types of negative effects. Overall, members of military organizations need to be vigilant for social engineering attempts. Additionally, cybersecurity experts need to focus on their training programs. Joe Ferrera writes, “Organizations must go beyond awareness initiatives and help end users actually make good security decisions and improve their cyber-hygiene.” This is true, and will help users both at work, to keep military networks safe, but also at home to safeguard other social media, email, and Internet security. In an article titled “Social Engineering Attacks” from Digital Guardian features Stu Sjouwerman and Kevin Mitnick on social engineering. They refer to a foundational principle for users: “Think Before You Click.” I believe there is a step, or a mindset, that needs to be instilled into employees that goes deeper than just “think before you click” and that is suspicion. Whenever employees face an unfamiliar situation, receive unsolicited or unverified contact (phone call or email), the first reaction should be suspicion. This will help users to think before they click but also take steps to verify the sender or take a few extra steps to investigate the legitimacy of the message, phone call, or website. As stated before, this behavior will help to guard users against threats in all contexts, not just while checking their email.

Charles Cooper provides a brief, but packed article covering three broad areas of a cloud security strategy. One big take away for the military should be the risks of employing both cloud capabilities and traditional data center capabilities because it could lead to gaps in security that were not there before. This “piecemeal” approach is already being executed within several large organizations in both the Air Force and DoD (Cooper, Section 2). The first large category is layered security. While Cooper hits on many aspects of a layered security, one emerging issue for the military is mobile security. The military needs to be cognizant of the changes required to secure mobile technology, as well as the transitory nature of mobile technology, as the name implies. Mobile assets are more difficult to connect, especially for those who travel frequently and may be more susceptible to Wi-Fi or Bluetooth attacks. The second strategy is data privacy. This is where a great partnership with your cloud service provider can create an advantage. Backup and encryption strategies, in particular, should be examined carefully to protect the data that is most important to the organization. For the military context, I believe we need to improve how we could execute elevated data security for certain connections at certain times to ensure military missions. The last area of strategy discussed is accountability for the cloud service provider. One key aspect of this is to identify what to do in the case of a breach. This is one area that has not been heavily explored by the military but should be in the near future. We need to trust and rely on proven cloud service providers because they can bring the cutting edge of security to our services. However, it is important to document the expectations and include mechanisms for accountability. Cloud security strategy is a hot issue right now, one that the US Army is also focused on, as highlighted by C4ISRNET (<https://www.c4isrnet.com/it-networks/2018/08/07/heres-a-look-at-the-armys-new-enterprise-cloud-strategy/>)