University of Nebraska Omaha

Space and Defense

Volume 12
Number 3 *Volume 12 Issue 2 (Summer 2021)*

Article 10

June 2021

Book Review: Aaron F. Brantly, The Cyber Deterrence Problem (Rowman & Littlefield International, Ltd. 2020), 202pp.

Yen Huynh
University of Nebraska at Omaha, yen.huynh@edu.edu

Book Review

Aaron F. Brantly, *The Cyber Deterrence Problem* (Rowman & Littlefield International, Ltd., 2020), 202 pp.

Yen Huynh

The usage of cyberwarfare has become increasingly prevalent in the global landscape, but there remains a lack of cohesive strategies and policies surrounding cyber deterrence. Aaron Brantly and a team of scholars specializing in different disciplines team up to develop the outline for a robust deterrence strategy concerning cyberspace. Brantly is an Assistant Professor of Political Science at Virginia Tech. He is also a Senior Research Scientist at the Army Cyber Institute at the United States Military Academy, West Point. In his book, he proposes different approaches that can and should be utilized to enhance deterrence in cyberspace.

The Cyber Deterrence Problem is best suited for scholars and those with at least a basic level of understanding regarding what cyberwarfare is. The arguments and concepts discussed in the book can be difficult to understand otherwise. The book looks to define what cyber deterrence is and develop a robust framework for policymakers to be able to reference the creation of cyber deterrence methods and policies. Cyberspace is the domain of global networks of technology infrastructures, telecommunication networks, and computer processing systems. Cyberwarfare is the use of digital attacks to cause damage or disrupt a country's computer system. The authors argue that the world of cybersecurity is quickly evolving, and states are scrambling to create strategies of prevention and response methods against cyber threats. This is what cyber deterrence centers around. As such, the United States needs to keep up with the adoption of new cyber deterrence policies to match the escalating threat levels. It is here where Brantly and his contributors try to make a splash. They posit that the United States needs to advance the current interest and government involvement in the creation and implementation of cyber deterrence methods.

Cyberspace is an ever-changing world, and though it lies below the nuclear threshold, threats of force are still common. Even so, the credibility of such threats varies, and they are rarely carried out. Unlike in the physical world, where deterrence is aimed at fighting physical targets, deterrence in cyberspace is different. Rather, it is directed against manipulations of elements of cyberspace and those engaging there. It is here that Brantly says the focus needs to shift if the United States is to keep our technological infrastructure safe. To sufficiently understand the threats and the different methods in creating a credible framework, the book utilizes approaches from different relevant fields to create better cyber deterrence strategies. By employing a multidisciplinary approach to the study of cyber deterrence, the book attempts to create a more comprehensive framework of strategies.

Classic deterrence centers on the potential adversary's cost-benefit analysis to see if their actions will elicit a response in the form of force. This is problematic because classic deterrence also sees that the defending states threaten the use of force or power but do not end up using them. Modern formulations of deterrence are mostly grounded on the concept of nuclear weapons and other traditional means of military weaponized interventions. In the cyberspace world, two main types of deterrence are commonly referenced. Deterrence by punishment and deterrence by denial are both intended to manipulate the cost-benefit analysis of an adversary. That is to say that an adversary is likely to change their calculations depending on the type of deterrence that the defending state is most likely to use. Deterrence is not yet well developed in the cyber world and can also be complex to understand and establish. The definitions of the two types of deterrence are defined multiple times, which could be confusing. Instead, it was a good way to remind readers of what deterrence by punishment and denial are.

Generally, deterrence by punishment focuses on the employment of threats to let adversaries know the costs of their unacceptable actions. On the other hand, deterrence by denial relies on the threat of denying the adversary the ability to achieve military and political gains through aggression. Deterrence by denials also attempts to convince attackers that their cyberattack will be more likely to fail than succeed, which makes the cost of trying not worth it. Successful deterrence can only occur when the potential adversary decides against carrying out the cyberattack due to the fear of punishment or the high possibility of failure.

To be successful, cyber deterrence policies should exhibit three critical features. The mechanisms 1) must successfully signal to the adversary the costs, 2) locate any present threats that exist in the cyber domain, and 3) cyber deterrence strategies should avoid utilizing nuclear analogy. As cyberattacks rank as the second-most-cited threat, the United States needs to move the deterrence framework forward. As the authors argue, the three prior mentioned components are essential in creating more secure cyberspace. The United States must clearly state what the punishments will be but also be able to swiftly identify cyber intruders. The book claims that the most difficult aspect is perhaps the need to rewire the brain to think about cyberwarfare in different terms as opposed to the kinetic or nuclear world. Even so, are the differences so vast that states must rethink their whole deterrence framework? Brantly does not provide evidence for this. It would be extremely helpful for readers to understand why he believes this to be an important consideration, especially when some of his readers may very well be involved in the decision-making of cyber deterrence policies and strategies.

Brantly and his co-authors try to drive the idea about the difference in the employment and responses of cyberspace and nuclear usage. The book claims that it is still possible for states to cross domains and utilize military force when responding

to cyberattacks. This is likely to happen if the cyberattack were deemed to pass a threshold of high salience and therefore elicits such a response. This makes it hard to fully understand the line between cyberattacks and military force or nuclear usage. When a cyberattack undermines active military operations or disables critical infrastructures, a cross-domain response will be more likely. This is especially so if the cyberattack threatens a state's homeland security system. In conjunction with cross-domain engagement, this also pushes forth the idea that states will utilize both the means of cyberattacks and military force when they are the aggressor and not just on the defense. The book fails to consider the impact of this.

It should be noted that anyone can involve themselves in cyberspace. There is a learning curve but once past it, the number of potential attackers increases. This refers to both state and non-state actors. As mentioned, multiple times throughout the book, the authors do remind readers that costs for adversaries in cyberspace are commonly lower than in the kinetic realm. The benefits can vastly vary depending on the goal of the attacker. In addition, it must be more challenging for the state being attacked to positively identify the attacker. Many cyberattackers can efficiently avoid detection and even when attacks are identified, finding the perpetrator remains an arduous task.

Due to the level of destruction that nuclear weapons can cause, they are seen as a weapon of last resort. The book claims that, consequently, cyberwarfare engagements are likely to continue as a first-step procedure. Other forms of military technology and interventions will be utilized when states know that a cyberattack is unlikely to accomplish what is needed. As previously mentioned, this assumption is to say that the United States and other governments do not think about employing both cyberattacks and military interventions, either to respond to attacks or when trying to accomplish something. Cyber-retaliation may be the cheaper method but is not always the most effective.

It can be hard to fully gauge the reasons behind a cyberattack. The more a state engages in invasive intelligence via cyberspace, the likelier their actions will be misinterpreted. In trying to read the reasonings behind attacks carried out in cyberspace, there are limits to what can be explained. The costs of cyberattacks and cyberwarfare are generally low. It can prove difficult to create successful overarching deterrence policies. Typically, cyber aggressors will keep trying to probe the system until they can find an entry point and successfully carry out their mission. As such, there are limitations to deterrence. Even though the authors have mentioned this fact, the book persists in claiming that deterrence is a necessary measure. If deterrence has limitations, then other methods should also be applied to increase the cybersecurity measures. Towards the end, the book does incorporate norms as a part of the cyber-deterrence discussion. While it is a worthwhile effort, previous chapters already reference this though not specifically referring to it as cyber norms.

Consequently, the book and co-authors can expand on the limitations of the cyber-deterrence strategies and what other realistic strategies could be included.

The book states that deterrence by punishment is less likely to be effective due to the high levels of uncertainty in identifying the attackers and the assets that are at risk. Clear signaling of costs can help establish the foundation for deterrence by punishment. The issue is that most cyberattacks exist below the threshold that is necessary to trigger punishment, which is why it is the less effective form of deterrence. As such, deterrence by denial should be strongly considered. Brantly and his co-contributors have expanded the platform for deterrence considerations. The methods explained in the book can showcase the importance of having a comprehensive framework on cyber deterrence. The over-arching framework that the book for the argument of cyber deterrence is thorough but not exhaustive. The complex details are laid out in a detailed and easy-to-understand manner once you have a basic understanding of cyberspace, cyberwarfare, and cyber deterrence.

Brantly offers a broad overview of the topic of cyber deterrence. He makes a solid argument as to why it is a necessity. Readers will understand why the United States needs to keep up with the strategic framework on cyber deterrence and what some of the potential approaches towards policy implementation can be. Readers should take note that there are some limitations. As previously mentioned, cyber deterrence is not going to solve all the problems that the United States encounters in cyberspace. Brantly and his fellow contributors do not do much to build on providing other methods that can be used in conjunction with cyber deterrence to strengthen the country's cybersecurity measures. Even so, *The Cyber Deterrence Problem* will help readers understand the importance of cyber deterrence and what some of the basic approaches are.

*Yen Huynh attended the University of New Mexico and graduated with a degree in Political Science and Criminology. She has experience working in campaigns and the New Mexico Legislature. She currently attends the University of Nebraska at Omaha and is a graduate assistant in the Political Science department. As a graduate assistant, one of her projects includes the role of managing editor for the Space & Defense journal. As a student, her research interests includes the civic and political engagement of Asian-Americans and the intergenerational study of Asian-Americans and Pacific Islander political experiences and identity.