The Limitation of United States Deterrence Strategy Towards North Korean Cyber Attacks

Kukuh Ugie Sembodho, Agus Trihartono & Abubakar Eby Hara
Universitas Jember

Abstract

This paper tries to discuss the development of cyberwar that threatens many countries by referring to the example of the North Korean cyberattack against the United States (US). Cyberattack is a relatively new phenomenon that many countries have not been able to anticipate adequately because it is difficult to track down and find the actors behind it. So far, countries have frequently accused each other of these attacks, but it is difficult to retaliate or anticipate due to unclear evidence. Unlike conventional warfare, no cyberattack warfare norms had previously been developed, nor had there been any attempt made in that direction. One thing that can be done in such a condition is the development of technology that is not only able to ward off the attack but, as stated in the theory of deterrence, can also provide a deterrent effect on the attacking country. By referring to the case of North Korea's attack on the US, we see that even a country as great as the US has not been able to develop a successful deterrence.

Keywords: *deterrence, cyberspace, cybersecurity, United States, North Korea*

Tulisan ini membahas mengenai perkembangan perang siber yang menjadi ancaman utama bagi banyak negara hari ini, dengan fokus pada serangan siber Korea Utara kepada Amerika Serikat (AS). Serangan siber merupakan fenomena yang relatif baru, sehingga banyak negara belum mampu untuk mengantisipasi hal tersebut karena sifatnya yang susah untuk dilacak dan susah untuk mengetahui aktor dibalik serangan tersebut. Sejauh ini negara tertentu seringkali dituduh menjadi dalang serangan siber, namun bukti yang seringkali tidak jelas membuat langkah antisipasi atau retaliasi menjadi sulit. Berbeda dengan perang konvensional, hingga saat ini belum ada norma serangan siber yang terbangun, bahkan pembicaraan mengenai hal tersebut cenderung minim. Sejalan dengan hal itu maka dalam perang siber dibutuhkan pengembangan teknologi yang tidak hanya mampu untuk menangkal serangan tapi juga memberikan efek deterrence *bagi negara penyerang. Dengan merujuk pada kasus serangan siber Korea Utara kepada Amerika Serikat, kita dapat melihat bahwa negara sekuat Amerika sekalipun ternyata belum mampu membuat mekanisme* deterrence *dalam serangan siber.*

Kata-kata kunci: Deterrence*, Ruang Siber, Keamanan Siber, Amerika Serikat, Korea Utara*

Cyberwars are becoming more frequent. One of many cyber attacks that have taken place in the past few decades is the attack allegedly carried out by North Korea against the United States (US). Aside from its nuclear power, North Korea also has capabilities in the cyber field. North Korea is one of four countries threatening the United States in cyberattacks (Coats 2018, 5). Some security experts even say that North Korea's cyber strength is more robust than Russia's (Hern 2018). Pyongyang is believed to have resources that can be used to provide a variety of offensive approaches with little or no warning, including cyber attacks, data deletion, and the spread of ransomware (Busby 2018).

North Korea has carried out various cyberattacks, including the Fourth of July Incident in 2009, Sony Pictures in 2014, and WannaCry in 2017 (Bing & Lynch 2018; Busby 2018). The impact of the cyberattack cannot be underestimated. On the Fourth of July Incident, cyber attacks succeeded in making various government websites crippled. Some websites that were successfully hacked during the attack include the United States Treasury, Secret Intelligence Service, United States Department of Transportation, US Securities and Exchange Commission, and various major media in the United States. During the attacks, hackers use Distributed Denial of Services (DDoS), which rendered the hacked website crippled (Castro 2009; Shaer 2009). Cyberattacks on Sony Pictures are equally dangerous. Guardians of Peace (GOP) successfully hacked the company and leaked various data such as e-mails among employees to several films that had not yet aired (Siboni & Siman-Tov 2014, 1). Although Sony Pictures is a private company, the cyber attacks' success shows how the cybersecurity system is lacking. Not only attacks that focus on the United States, the impact of the WannaCry ransomware successfully terrorized more than 150 countries. This attack is a world lesson on how cyber attacks can significantly affect a state or even the world. Several sectors, such as health and education, were paralyzed in the attack's aftermath (Department of Health/DoH 2018, 11).

How America can fight and anticipate the possibility of further attacks from North Korea is the main topic of this paper. As a superpower, the US should be able to anticipate the attacks. The United States' position is ranked second or included in the Leading

Country category in the Global Cybersecurity Index (International Telecommunications Union/ITU 2018) and ranked first in the Cyber Attack Power Ranking by Country (Celiktas & Unlu 2018, 480). Both indexes at least describe how the United States has more than adequate defensive and offensive capabilities. Besides, the United States' position is also benefited from seeing its positive asymmetries (Kshetri 2014, 174). The most straightforward calculation can be seen from the US per capita national income, which reached USD 56,140, far more significant than North Korea, with around USD 583 in 2014 (United Nations 2014). If we use the classic deterrence strategy, the United States should have enough resources to ward off various cyberattacks.

The continuous attacks carried out by North Korea showed the lack of deterrence built by the United States. This research will then explain how the deterrence strategy shifts in the cyber realm and how it is applied in the United States and North Korea case. This paper is divided into four sections. First, the paper discusses the strategic value of cyberspace. Second, it elaborates on how cyberspace has become a new arena for fighting between countries. Third, it tries to see how deterrence theory deals with cyberwar. Fourth, it looks at the US's response, trying to develop deterrence against the cyberattack, and sees how it turns out.

The Strategic Value of Cyberspace

The Age of Information, which is often referred to as the digital era, is a historical period in the 21st century marked by a rapid shift from what was produced by the industrial era to a new economy based on information technology (Torr 2003, 20). The beginning of the Age of Information can be attributed to William Shockley, Walter Houser Brattain, and John Bardeen, inventors, and engineers of the first transistors who were the turning points for the modern technological revolution. Just as the Industrial Revolution, the digital revolution marked the Industrial Age's beginning (Ohmae 1995, 143). The definition of digital (or information) continues to change from time to time as new technologies, user devices, and methods of interaction with other humans are discovered.

In this context, we see technological advances in the cyber world that are getting faster. The word "cyber" was derived from cybernetics, which means "through the use of computers". Cyberspace terms include the combination of all communication networks, databases, and information sources into infinite space. Cyberspace can also be interpreted as a virtual and immaterial network ecosystem and a universal bio-electronic environment (Cavelty 2012, 155). Scholars, such as Matt Murphy (2010) of the Economist, consider cyberspace the fifth domain of warfare, after land, air, sea, and space. Even though it has started to be discussed a lot, no definition can describe cyberspace holistically. Due to the absence of an adequate explanation, there are often misunderstandings in defining cyberspace.

Physically, cyberspace consists of the hardware components used in building networks, such as routers, servers, and computers, and the infrastructure that allows these components to be connected, such as fiber optic cables, local area network (LAN) cables, or wireless technology. These hardware components are geopolitically defined and are usually subject to national jurisdiction. While often not included in the definition of cyberspace, in the context of national security, some countries will also consider enabling infrastructures such as telecommunications systems and power grids. This hardware component is connected in a network with software components that allow information to be sent and received in packets according to network protocols, such as the ISO / OSI Reference Model or the TCP / IP model (Kuehl 2009, 9).

The functional description of cyberspace is still being debated in various countries and organizations. In the most basic sense, cyberspace is concerned with information in or transferred through networked computer systems and human interactions with other humans or communication through this network. From these definitions, countries or organizations have different ideas about activities in and through cyberspace that must be regulated and controlled. Some will describe cyberspace as merely a network environment, emphasizing infrastructure and connectivity. In contrast, others will explicitly include the importance of cyberspace's information content in their definition, which then serves to regulate or influence related concepts such as intellectual

property, freedom of expression, and privacy (Hathaway & Klimburg 2012, 9). Despite these differences, both content and environment are considered critical functional features of cyberspace for this paper.

Some of the main characteristics of cyberspace make it different from other domains. First, cyberspace allows users to transmit large amounts of information efficiently and quickly. Communication is not just point-to-point or broadcast but uses packet switching. Information also consists of small blocks based on the destination address and then sent over multiple lines. This feature allows for a new paradigm of information exchange. Second, users have enjoyed anonymity so far. Many network systems, including the Internet, have not been designed with security or identity in mind. Apart from several identification features such as the I.P. address and media access control address, it is often difficult to trace the cyberspace activity source. It is also challenging to establish a relationship between a person's physical/legal identity and their person in cyberspace. Recently, however, various tools and techniques have emerged to manage attribution problems better. The attribution issue's level of importance varies depending on the actor and the type of cyber activity being carried out (House Science and Technology Committee 2010). However, due to general trends, attribution is still time-consuming, expensive, and often requires collaboration between authorities in different countries. Third, unlike other operational domains, cyberspace is a human-made domain in which many hardware and software building blocks can be modified and reconfigured. This means that networks and systems can be rebuilt and redesigned in more than one way, depending on their priorities and needs.

Threats to Cyberspace

Under these conditions, perhaps we can start to assume that who controls cyberspace will rule the world. This proposition means that the war strategy must change or anticipate how to deal with the possibility of cyberwar. Policymakers, military institutions, and other non-governmental actors were examining the effective ways to deal with what is then known as cyberwar. Unlike past

weapons, the technology needed to start a cyberwar is not limited to a person/group of actors in a system. The ability to attack a vital system can be carried out by both the state and non-state, both of which can disrupt the society that depends on information.

In recent years the world has seen clear evidence of cyber warfare. The attacks include the 2007 cyber attack in Estonia, the 2008 attack in Georgia, the 2009 Stuxnet virus that attacked Iran's nuclear program, and actions by the "Anonymous" hacker group against Visa, Mastercard, PayPal, and Amazon via Wikileaks. Each attack represents the potential devastation that cyber warfare can do. Since cyberwar is an unconventional and asymmetrical war, countries that are weak in conventional military power also tend to invest in balancing traditional forces (Geers 2011, 114). In this regard, policymakers will be asked to develop strategies that address cybersecurity issues. Many problems will compound the difficulty of developing an effective strategy. The issues are what qualifies as cyber warfare. Should the response be the same, whether the attack comes from state or non-state actors, does the state respond similarly when the civilian sector elements are threatened rather than the public sector offensive or defensive stance necessary?

While much has been written on the topic, there needs to be a more vigorous examination of how the combination of cyber weapons with traditional strategic approaches might influence cyber warfare strategic choices. Does the past warfare approach fit into the evolving context of cyber warfare, or should a new generation of strategists be developed to deal specifically with cyberwar ideas? Examining the possible application of the classic concepts of war to cyber-warfare must consider possible policy consequences based on the potential outcomes. While bombs or missiles may not be compatible with cyber warfare, this type of conflict's repercussions may be more devastating in disrupting society. In the context of cybersecurity, the more electronically dependent actors are, the more vulnerable they are (Liaropoulos 2011, 4).

As the world is changing, cybersecurity policies should have been developing both from their approach and implementation. However, in many cases, it is evident that the ideas of classic deterrence strategies, which are products of the World War and

Cold War-era, still dominate the cybersecurity policy-making process (Lewis 2018, 2). Theoretically, nuclear deterrence from the Cold War era can no longer answer the contemporary problems we face. Cyberspace is a new medium that, until now, has not been well mapped. Therefore, the approach taken should also be different.

The commercialization of the Internet in many fields makes its use should be maximized as much as possible. This makes global internet development very fast and unavoidable, which ultimately demands the state to secure cyberspace more than ever. Such rapid growth requires a re-actualization of several concepts related to cybersecurity. Unlike the other domain, cyberspace is intangible and has no boundaries; states and individuals have the same ability to carry out cyberattacks; one can even argue that individuals have greater power than the states. The blurry nature of cyberspace makes attribution to alleged individuals, groups, or even states harder. This condition could result in probably the most significant threat of cybersecurity, namely the attack of critical state infrastructure through cyberspace (Greathouse 2014, 22).

How to Overcome: The Deterrence Theory?

One of the methods developed to overcome the outbreak of war in conventional warfare is the deterrence theory. Deterrence is one of the studies in international relations that has a longstanding history. It can be traced down since Ancient Greece. In his seminal work, Professor Richard N. Lebow (2007, 20) explained the ten stories of Thucydides, who used deterrence and compellence strategies in the Peloponnesian War. In recent years, there has been a shift in the concept of deterrence as it develops over information technology development. The tragedy of 9/11, Estonian cyberattacks, and Stuxnet in Iran was considered a catalyst for cyber warfare discourse, followed by cyber deterrence by military experts (Kaiser 2015, 11).

Deterrence in international security studies refers to strategic efforts to prevent other parties from taking harmful actions by providing a picture of a counterattack should the activity is carried

out (Morgan 2010, 55). In other words, deterrence is an inducement to potential attackers by conveying that not carrying out an attack is the best decision to take (Morgan 1977, 22). The concept of deterrence refers to a form of deterrence effect that mainly relies on negative incentives (Paul, Morgan, & Wirtz 2009, 2). This strategy's existence is widely discussed by international relations scholars in the Cold War era. There was a nuclear arms race between the United States and the Soviet Union, which consisted of three components: capability, credibility, and communication.

As technology develops, the relationship between cyber warfare and deterrence strategies has increased and become the focus studies of several security experts. Many then search for answers on how to implement the classical deterrence theory to be later a solution for cyber attacks and cyber warfare that might occur (Lupovici 2011, 49-51). This discourse then becomes the origin regarding the emergence of what Goodman put forward, which is then called cyber deterrence theory.

The use of cyber deterrence strategies can be traced back to Operation Desert Storm in 1991, when the idea of a military revolution came under the spotlight. At the beginning of the attack, the United States launched an information war that D. Betz defined as a potential weapon in its own right (Betz 2006, 508) to the Iraqi government by paralyzing its military communication system. The incident then showed the importance of the cyber deterrence strategy. In the 1990s, experts provided a factual basis for deterrence and I.W. studies. After various cyberattacks in the late 2000s, such as cyber-attacks in Estonia in 2007, experts' attention turned to preventing cyberattacks or cyber warfare, which had strategic and political objectives (Stevens 2012, 149-151).

According to the explanation above, we will develop a cyber-deterrence framework using the classic deterrence theory, which uses two main strategies: deterrence by denial; and punishment or retaliation (Geers 2010, 7; Libicki 2009, 29).

Deterrence by Denial

In general, deterrence by denial is an attempt to prevent

potential aggressors from getting or achieving their goals through cyberattacks. This strategy seeks to show how various attacks will lead to unpleasant results (Kugler 2009, 327). This strategy aims to minimize opponents' chances to benefit by carrying out attacks through computer and network protection (Jasper 2015, 69). Thus, the purpose of deterrence by denial is the enemy's persuasion that, with a strong defense, the attack will not get benefits equivalent to the costs incurred (Philbin 2013, 25).

Deterrence by Punishment

The other primary strategy is deterrence by punishment or retaliation. This method is offensive (Goodman 2010, 106), which shows threats, losses, and significant risk should the country is attacked. The ultimate goal is to convince the enemy that there are potentially high retaliation probability and severity should the attack happen. As in classical deterrence theory, cyber deterrence demands immediate, definite, and severe punishment. In other words, the consequences of acts of retribution must be absolute or undeniable.

The emergence of the term cyber deterrence then raises the debate about the relevance of the virtual realm's classic deterrence strategy. On the one hand, as explained earlier, some scientists argue that the current deterrence strategy is still relevant and can be applied in cyberspace (Rice, Butts, & Shenoi 2011). On the other hand, the researchers questioned the classical deterrence theory's ability to answer cyber problems. They identified various technological, political, and legal factors in the cyber realm, which showed that the classical deterrence theory was no longer suitable for the application. These factors include technological volatility, anonymity, confusion, ambiguity, asymmetrical nature, and limitations on international law and norms. This distinctive feature of the cyber realm then forms a new pattern in achieving an effective deterrence strategy (Gartzke & Lindsay 2015, 320; Geers 2010; Kello 2013, 33; Lupovici 2011, 49-51).

Limitations of Deterrence Theory in Cyberwar

Based on the deterrence strategy above, the reason regarding the limitations of the United States deterrence strategy against the North Korean cyberattack rested on the characteristic that emerged along with the cyberspace itself. As a new domain in international conflicts, cyberspace provides various unique traits that force policymakers to reconfigure their national security systems. Some of the reasons below are the results of studies of some North Korean cyberattacks that succeeded in attacking the United States.

North Korea's successful cyber attacks against the United States illustrate the main obstacle to the cyber deterrence strategy: contestation. In the context of cybersecurity, contestation usually refer as confusion in terms of power, where the parameters of strength and power used in security studies are no longer absolute. The nature of cyber deterrence emerges as the result of three main properties of cyberspace, namely: anonymity, asymmetry, super empowerment.

Undoubtedly, anonymity is a significant obstacle to cyber deterrence strategies. Because the Internet is not equipped/developed with authentication of identity, attacks launched through cyberspace are ultimately dominated by anonymous attacks. Investigators must deal with anonymity every time a cyber-attack occurs to determine who is responsible for the attack. Although we can identify the origin of attack, there is also the possibility of it being a transit point. Many cyber attacks use transit points to create false flag operations to extend the attribution process (Taipale 2010, 21). Even if the investigator can verify the attacker's identity in the end, they will still face difficulties in revealing the offender's motives –whether the attacker is working alone, based on orders, or even accidentally attacking (Libicki 2009, 25-26).

In many cases, this investigation could take a long time and counterattack could be perceived as aggression rather than retaliation (Libicki 2009, 52). The attribution process's length indirectly makes the deterrence process in cyberspace less effective, considering that one of the prerequisites for adequate deterrence is to retaliate quickly. In sum, anonymity in cyberattacks will reduce

the possibility of the state to carry out retaliation, and if this is possible, the degree of effectiveness will undoubtedly decrease. Therefore, anonymity in cyberspace does pose a significant obstacle to cyber deterrence.

Cyber attacks carried out by North Korea against the United States also show asymmetry in cyberspace. Although the United States can attribute an attack to a particular country (e.g., North Korea), that doesn't mean that information can help the retaliation process because the target country may not feel the impact as harmful. The problem that arises here is that each state has a different degree of dependence on the internet network. The United States has a much higher reliance on the Internet than North Korea. This condition makes any form of retaliation carried out by the United States will not impact the damage caused by North Korean cyber attacks.

Finally, North Korea's cyberattack on the United States also illustrates how the Internet and cyberspace can create super-empowered actors. Although the United States has pointed to North Korea as the actor behind various cyberattacks, the Guardian of Peace (GOP) shows that even a group of hackers can be part of a cyberattack. In this case, if an individual or a group that only uses a personal computer can carry out cyber attacks on a country's critical infrastructure, then the individual or group becomes equal to the state in the cyberspace (Beeker 2009, 10-11). This condition certainly creates a new challenge for an effective cyber deterrence strategy. As explained earlier, the deterrence process in cyberspace against a country has faced many challenges. Therefore, it will be more difficult for the state to deter individuals or groups.

Scalability on Cyberspace

Based on the cyberattacks carried by North Korea to the United States, we can see how difficult it is to be able to achieve effective deterrence in cyberspace, especially related to scalability. Scalability closely connected to various possibilities that can occur due to an attack carried out in cyberspace. In the physical world, attack ability will be limited to the initial purpose of an attack. This means that both weapons are used and what impacts might occur are predictable (Taipale 2010, 19). For example, North Korea's ballistic missiles may be dangerous, but the effect they might have

can be predicted. The ability to predict/determine an attack's impact is essential in creating an effective deterrence process because it will relate to the retaliation measure.

In cyberspace, determining the impact of an attack is not easy. An attack can cause various effects that make the attack difficult to predict. For example, on the 4th of July cyber attacks, the North Korean Government succeeded in crippling several government sites down, which have an essential role in the United States' survival. The attack's impact is not just the paralysis of governmental websites but also the governmental system. For the United States, government sites are an essential asset considering that many government systems operate through the Internet. If a site is disabled, then the whole system that depends on the site will be disrupted.

Another example is the impact of WannaCry Ransomware. An attack that initially aimed to disrupt health and education sites, could have a severe domino effect. Although attacks can eventually be halted, within a short period WannaCry Ransomware succeeds in delivering a great message if cyberattacks can have a significant impact on the physical world if targeted strategically.

Scalability is thus proven to inhibit the process of forming an effective deterrence strategy (Kugler 2012, 338). Since an attack can lead to various impacts and the inability to predict these impacts, the message of deterrence should no longer focus on what action to do but rather what might be received if the state carried out a cyber attack. The inability to know the scale and purpose of enemy cyber activity will ultimately make it difficult to determine a compelling deterrence message.

Realizing these various cyberattacks, the United States did not remain silent. The United States is trying to develop a cybersecurity system to overcome or prevent similar attacks. The United States has begun to pay attention to cybersecurity since 2002 with the creation of The Homeland Security Act of 2002, which contains the Cyber Security Enhancement Act of 2002 (Department of Homeland Security/DHS 2002). After that, the discourse on cybersecurity continues to develop and produce various legal frameworks specifically governing cybersecurity. Such as the Cyber

Intelligence Sharing and Protection Act (CISPA); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (SECURE IT); the Cybersecurity Act of 2012; and the National Cyber Strategy 2018 (Tirrel 2012).

Temporality on Cyberspace

Another nature of cyberspace that hinders cyber deterrence, especially in the United States, is temporality. This trait refers to the fact that attacks carried out in cyberspace have an immediate nature (Blank, 2001: 143). In the physical world, the soon-to-be-attacked country has a chance to know the attacks to be carried out by the enemy. For example, in airstrikes or missiles, attacked countries can determine the imminent attack through a radar system. Satellite imagery could also identify this attack.

In the case of North Korea's cyberattack on the United States, we can see how there are limitations in predicting an attack. In contrast to attacks in the physical world, attacks in cyberspace through network surveillance, virus delivery, and DDoS gives limited information regarding when, how, to whom, and on what basis a cyberattack is carried out. For example, during the 4th of July Incident, the attack took place on U.S. Independence Day. In the middle of the celebration, who would have thought that a cyberattack would take place. Its sudden nature also makes deterrence difficult.

Conclusion

War and conflict in cyberspace is a new discourse for academics, government, and military experts. Because of the newness, countries are trying to find a middle ground related to how deterrence should be carried out in cyberspace. In addition to all the United States' efforts and its theoretically strong position, the United States is currently faced with unique characteristics that emerge in cyberspace. Some problems related to the difficulty of attribution of cyber attacks, the nature of asymmetry, the

emergence of super-empowered individuals, the various impacts of a cyber attack, and sudden attacks are considered factors that influence the limitations of the United States.

References

Book and Book Chapter

Blank, Stephen, 2001. "Can Information Warfare be Deterred?" in Albert, D. S., & Papp, D. D. (ed.), *Information Age Anthology, Volume III: The Information Age Military*. Washington, DC: Command and Control Research Program.

Cavelty, Dunn M., 2012. "Cyber Security". In Collins (ed.), *Contemporary Security Studies*. New York: Oxford University Press.

Geers, K., 2011. *Sun Tzu and Cyberwar*. Cooperative Cyber Defence Centre of Excellence.

Hathaway, M. E., & Klimburg, A., 2012. "Cyber Terms and Definition" in Klimburg, A. (ed.), *National Cyber Security Manual*. Tallinn: NATO CCD COE Publications.

Kshetri, N, 2014. *The Quest to Cyber Superiority*. Springer.

Kuehl, Daniel T. 2009. "Chapter 2: From Cyberspace to Cyberpower: Defining the Problem". In Kramer, F. D. et.al. (ed.), *Cyberpower and National Security*. Washington, DC: National Defense University.

Kugler, R. L., 2012. "Deterrence of Cyber Attacks" in Kramer, F.D., et.al (ed.), *Cyber Power and National*. Lincoln: University of Nebraska Press.

Libicki, M. C., 2009. *Cyber Deterrence and Cyberwar*. Santa Monica: RAND Corporation.

Morgan, P. M., 1977. *Deterrence: A conceptual analysis*. Beverly Hills, CA: SAGE Publications.

Morgan, P. M. 2010. "Applicability of traditional deterrence concepts and theory to the cyber realm" in *Proceedings of a*

workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy.

Ohmae, Kenichi, 1995. *The End of the Nation State: The Rise of Regional Economies*. New York: The Free Press.

Taipale, K., 2010. "Cyber-deterrence" in Reich, P. C., & Gelbstein, E. (ed.), *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization*. Hershey: IGI Global.

Torr, James D., 2003. *The Information Age*. Michigan: Greenhaven Press.

Journal & Online Journal

Adams, James, 2001. "Virtual Defense", *Foreign Affairs*, **80**(3): 98-112. DOI: 10.2307/20050154

Barnett, Roger W, 1998. "Information Operations, Deterrence, and the Use of Force", *Naval War College Review,* **51**(2).

Gartzke, E., & Lindsay, J. R., 2015. "Weaving tangled webs: Offense, defense, and deception in cyberspace", *Security Studies*, **24**(2) 316–348 https://doi.org/10.1080/09636412.2015.1038188

Geers, K., 2010. "The challenge of cyber attack deterrence", *Computer Law & Security Review*, **26**(3): 298–303 https://doi.org/10.1016/j.clsr.2010.03.003

Goodman, W. 2010. "Cyber deterrence: Tougher in theory than in practice?" *Strategic Studies Quarterly*, 4(3): 102–135.

Jasper, S., 2015. "Deterring malicious behavior in cyberspace", *Strategic Studies Quarterly 2*, **9**(1): 60–85.

Kaiser, R., 2015. "The Birth of Cyberwar", *Political Geography*, **46**(1): 11–20 https://doi.org/https://doi.org/10.1016/j.polgeo.2014.10.001

Kello, L., 2013. "The meaning of the cyber revolution: Perils to theory and statecraft" *International Security*, **38**(2): 7–40 https://doi.org/10.1162/ISEC_a_00138

Lebow, R. N., 2007. "Thucydides and Deterrence", *Security Studies* **16**(2): 163-188. http://dx.doi.org/10.1080/09636410701399440

Lupovici, A., 2011. "Cyberwarfare and deterrence: Trends and challenges in research", *Military and Strategic Affairs*, **3**(3).

Rice, M., et.al., 2011. "A signaling framework to deter aggression in cyberspace" *International Journal of Critical Infrastructure Protection*, **4**(2): 57–65. https://doi.org/10.1016/j.ijcip.2011.03.003

Reports

Coats, D., 2018. *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*.

Siboni, G., & Siman-Tov, D., 2014. *Cyberspace Extortion: North Korea Versus the United States*.

U.S. Energy Information Administration, 2010. "Country Analysis Brief-India" [online]. in http://www.eia.doe.gov/cabs/India/Full.html [accessed on 22 October 2010].

Liaropoulos, A., 2011. "Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict". GPSC working paper.

Online Articles

Bing, C., & Lynch, S., 2018. "U.S. charges North Korean hacker in Sony, WannaCry cyberattacks" [online] in https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W . [Accessed on 28 October 2020]

Busby, M., 2018. "North Korean hacker charged over cyber attacks against NHS" [online] in https://www.theguardian.com/world/2018/sep/06/us-doj-north-korea-sony-hackers-chares [Accessed on 2 October 2020]

Castro, D., 2009. "Thoughts on 4th of July Cyber Attacks" [online] in https://www.innovationfiles.org/thoughts-on-4th-of-july-cyber-attacks/ [Accessed on 8 October 2020]

Hern, A., 2018. "North Korea is a bigger cyber-attack threat than Russia, says expert" [online] in https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia [Accessed on 21 October 2020]

Murphy, M. 2010. "War in the Fifth Domain" [online] in https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain [Accessed on 28 October 2020]

Philbin, M. J., 2013. "Cyber deterrence: An old concept in a new domain" [online] in http://oai.dtic.mil/... [Accessed on 28 October 2020]

Shaer, M., 2009. "North Korean hackers blamed for sweeping cyber attack on U.S. networks" [online] in https://www.csmonitor.com/Technology/Horizons... [Accessed on 26 October 2020]

Thesis

Beeker, Kevin R., 2009. *Strategic Deterrence in Cyberspace. Thesis.* Ohio: Air Force Institute of Technology.

Tirrel, W., 2012. *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?*. Thesis. Kansas: The George Washington University.